Remote Supervisor Adapter II SlimLine
and Remote Supervisor Adapter II

User's Guide

Remote Supervisor Adapter II SlimLine
and Remote Supervisor Adapter II

User's Guide

Note: Before using this information and the product it supports, read the general information in Appendix B, “Notices,” on page 115.

Seventh Edition (April 2007)

Contents

Chapter 1. Introduction

This document explains how to use the functions of the IBM® Remote Supervisor Adapter II SlimLine and the IBM Remote Supervisor Adapter II when they are installed in an IBM server. The Remote Supervisor Adapter II SlimLine and the Remote Supervisor Adapter II provide the following functions:

- Around-the-clock remote access and system management of your server.
- Remote management independent of the status of the managed server
- Remote control of hardware and operating systems
- Web-based management with standard Web browsers

Note: Throughout this document, the term *Remote Supervisor Adapter II* is used to denote both the Remote Supervisor Adapter II SlimLine and the Remote Supervisor Adapter II, unless otherwise noted.

If firmware and documentation updates are available, you can download them from the IBM Web site. The Remote Supervisor Adapter II might have features that are not described in the documentation that comes with the adapter, and the documentation might be updated occasionally to include information about those features, or technical updates might be available to provide additional information that is not included in the adapter documentation. To check for updates, complete the following steps.

Note: Changes are made periodically to the IBM Web site. Procedures for locating firmware and documentation might vary slightly from what is described in this document.

1. Go to http://www.ibm.com/systems/support/.
2. Under **Product support**, click **System x**.
3. Under **Popular links**, click **Software and device drivers** for firmware updates, or click **Publications lookup** for documentation updates.

Important:

- To avoid system problems due to firmware differences, do not move a Remote Supervisor Adapter II from one server type to another server type. For example, do not move a Remote Supervisor Adapter II from an IBM System x3500 server to an IBM System x3850 server.
- If a Remote Supervisor Adapter II SlimLine is installed in an xSeries 366 server, when you turn on the server for the first time after the adapter is installed, the server might appear to be unresponsive for an unusual length of time (up to 10 minutes). If this happens, when the server completes POST, flash the BIOS and baseboard management controller (BMC) firmware to the latest available levels. Then, flash the Remote Supervisor Adapter II SlimLine firmware. For more information, go to http://www.ibm.com/support/ and search for MIGR-59095.

Remote Supervisor Adapter II features

The Remote Supervisor Adapter II has the following standard features:

- Access to critical server settings
- Access to server vital product data (VPD)
- Advanced Predictive Failure Analysis® (PFA) support

- Alphanumeric or numeric pager alerts (not supported with the Remote Supervisor Adapter II SlimLine)
- Automatic notification and alerts
- Automated Server Restart (ASR)
- Continuous health monitoring and control
- Domain Name System (DNS) server support
- Dynamic Host Configuration Protocol (DHCP) support
- E-mail alerts
- Enhanced user authority levels
- Event logs that are time stamped, saved on the Remote Supervisor Adapter II, and can be attached to e-mail alerts
- Independent power, which enables around-the-clock access to the server even when the server power is off
- Advanced System Management (ASM) interconnect remote access (not supported with the Remote Supervisor Adapter II SlimLine)
- Operating-system-failure screen capture
- Remote access through Ethernet and ASM interconnect peer-to-peer network
- Remote disk enabling the attachment of a diskette drive, CD-ROM drive, USB flash drive, or disk image to a server
- Remote firmware update and access to critical server settings
- Remote power control
- Seamless remote accelerated graphics
- Secure Web server user interface
- Server console redirection.

  This feature is not supported with the Remote Supervisor Adapter II SlimLine when it is installed in any of the following servers:
  - IBM xSeries 236
  - IBM xSeries 260
  - IBM xSeries 336
  - IBM xSeries 346
  - IBM xSeries 366
  - IBM xSeries 460
  - IBM System x3800
  - IBM System x3850
  - IBM System x3950
- Simple Network Management Protocol (SNMP) support
- Remote firmware update
- User authentication using a secure connection to a Lightweight Directory Access Protocol (LDAP) server

Web browser and operating-system requirements

The Remote Supervisor Adapter II Web interface requires the Java™ Plug-in 1.4 or later and one of the following Web browsers:

- Microsoft® Internet Explorer version 5.5 or later with the latest Service Pack
- Netscape Navigator version 7.0 or later
- Mozilla version 1.3 or later (Remote Control features are supported only on the Remote Supervisor Adapter II SlimLine with Refresh 2 firmware.)

Note: The Remote Disk feature works with only the Microsoft Windows 2000 and Windows XP operating systems (for the Remote Supervisor Adapter II only, not the Remote Supervisor Adapter II SlimLine).

The following server operating systems have USB support, which is required for the Remote Control feature:

- Microsoft Windows® Server 2003
- Microsoft Windows 2000 with Service Pack 4 or later
- Red Hat Linux version 7.3
- SUSE Linux version 8.0
- Novell NetWare 6.5

Note: The Remote Supervisor Adapter II Web interface does not support the double-byte character set (DBCS) languages.

Notices used in this book

The following notices are used in the documentation:

- **Notes:** These notices provide important tips, guidance, or advice.
- **Important:** These notices provide information or advice that might help you avoid inconvenient or problem situations.
- **Attention:** These notices indicate potential damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage could occur.

Chapter 2. Opening and using the Web interface

To access the Remote Supervisor Adapter II remotely using the Remote Supervisor Adapter II Web interface, you must log in to the adapter. This chapter describes the login procedures and describes the actions you can perform from the Remote Supervisor Adapter II Web interface.

Logging in to the Remote Supervisor Adapter II

To access the Remote Supervisor Adapter II through the Remote Supervisor Adapter II Web interface, complete the following steps:

1. Open a Web browser. In the address or URL field, type the IP address or host name of the Remote Supervisor Adapter II to which you want to connect.

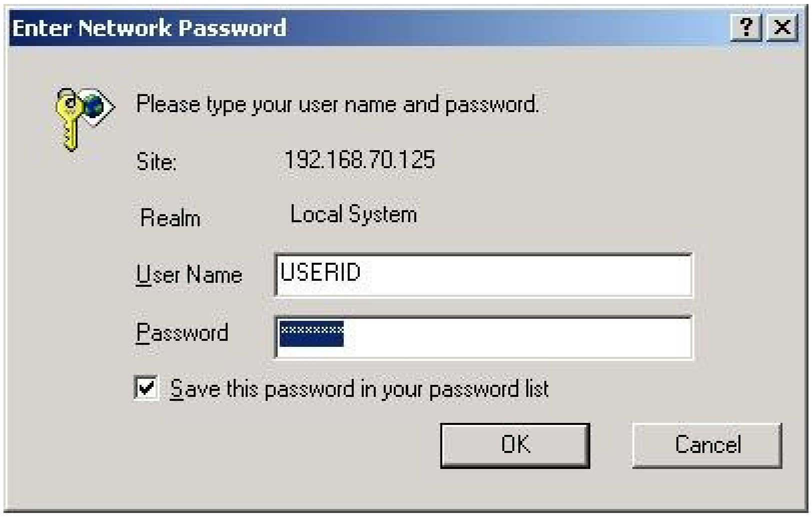
   Notes:

   a. If you are logging in to the Remote Supervisor Adapter II for the first time after installation, the Remote Supervisor Adapter II defaults to DHCP. If a DHCP host is unavailable, the Remote Supervisor Adapter II uses the default static IP address 192.168.70.125.

   b. You can obtain the DHCP-assigned IP address or the static IP address from the server BIOS or from your network administrator.

   The Enter Network Password window opens.

   Note: The values in the following window are examples. Your settings will be different.



Please type your user name and password.

Site: 192.168.70.125

Realm Local System

User Name USERID

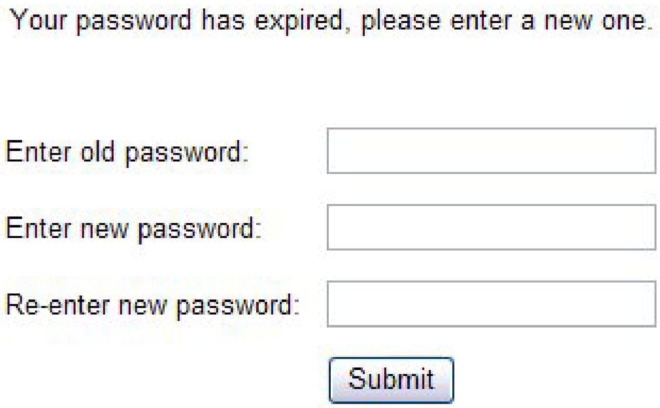
Password ********

☑ Save this password in your password list

2. Type your user name and password in the Enter Network Password window. If you are using the Remote Supervisor Adapter II for the first time, you can obtain your user name and password from your system administrator. All login attempts are documented in the event log. A welcome page opens in your browser.

   Note: The Remote Supervisor Adapter II is set initially with a user name of `USERID` and password of `PASSW0RD` (with a zero, not the letter O). This user has read/write access. Change this default password during your initial configuration for enhanced security.

3. Depending on how your system administrator has configured the user ID, the following window might open.



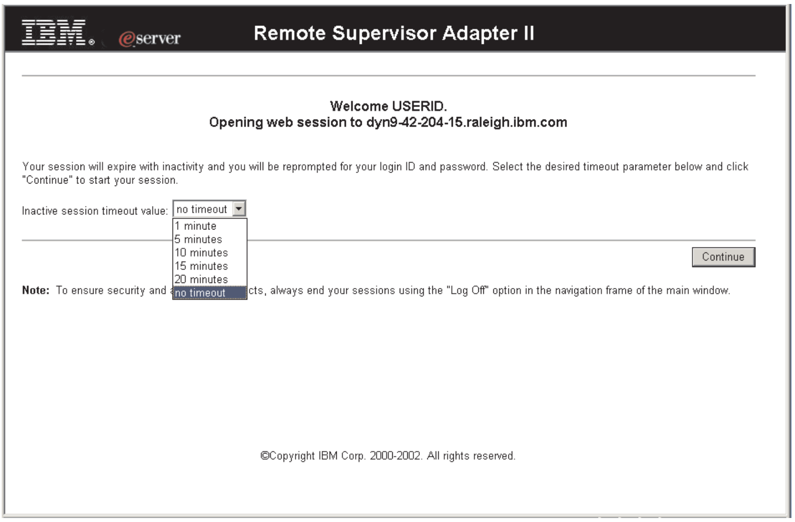
Your password has expired, please enter a new one.

Enter old password:

Enter new password:

Re-enter new password:

4. The Welcome window opens.



Welcome USERID.
Opening web session to dyn9-42-204-15.raleigh.ibm.com

Your session will expire with inactivity and you will be reprompted for your login ID and password. Select the desired timeout parameter below and click "Continue" to start your session.

Inactive session timeout value: no timeout

Note: To ensure security and a cts, always end your sessions using the "Log Off" option in the navigation frame of the main window.

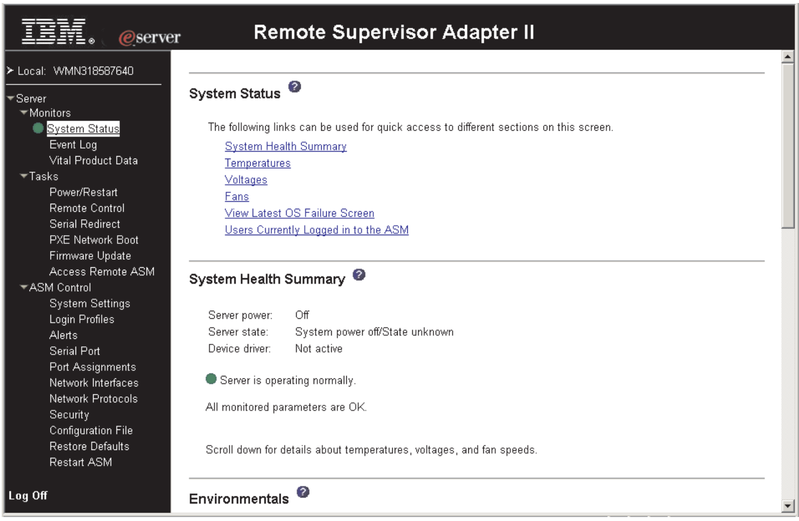
©Copyright IBM Corp. 2000-2002. All rights reserved.

Select a timeout value from the drop-down list in the field that is provided. If your browser is inactive for that number of minutes, the Remote Supervisor Adapter II logs you off the Remote Supervisor Adapter II Web interface.

Note: Depending on how your system administrator has configured the global login settings, the timeout value might be a fixed value.

5. Click **Continue** to start the session.

   The browser opens the System Status page, which gives you a quick view of the server status and the server health summary.



System Status

The following links can be used for quick access to different sections on this screen.

System Health Summary
Temperatures
Voltages
Fans
View Latest OS Failure Screen
Users Currently Logged in to the ASM

System Health Summary

Server power:	Off
Server state:	System power off/State unknown
Device driver:	Not active

● Server is operating normally.

All monitored parameters are OK.

Scroll down for details about temperatures, voltages, and fan speeds.

Environmentals

For descriptions of the actions that you can perform from the links in the left navigation pane of the Remote Supervisor Adapter II Web interface, see "Remote Supervisor Adapter II action descriptions" on page 8. Then, go to Chapter 3, "Configuring the Remote Supervisor Adapter II," on page 11.

Remote Supervisor Adapter II action descriptions

Table 1 lists the actions that are available when you are logged in to the Remote Supervisor Adapter II.

Table 1. Remote Supervisor Adapter II actions

Link	Action	Description
System Status	View system health for a server, view the operating-system-failure screen capture, and view the users who are logged in to the Remote Supervisor Adapter II	You can monitor the server power and state and the temperature, voltage, and fan status of your server on the System Health page. You can also view the image of the last operating-system-failure screen capture and the users who are logged in to the Remote Supervisor Adapter II.
Event Log	View event logs for remote servers	The Event Log page contains entries that are currently stored in the server event log and power-on self-test (POST) event log. Information about all remote access attempts and dial-out events are recorded in the event log. All events in the log are time stamped using the Remote Supervisor Adapter II date and time settings. Some events will also generate alerts, if configured to do so on the Alerts page. You can sort and filter events in the event log.
Vital Product Data	View the server VPD	When the server starts, the Remote Supervisor Adapter II collects system information, basic input/output system (BIOS) information, and server component vital product data (VPD) and stores it in nonvolatile memory. This data is available from the Vital Product Data page.
Power/Restart	Remotely turn on or restart a server	The Remote Supervisor Adapter II provides full remote power control over your server with power-on, power-off, and restart actions. In addition, power-on and restart statistics are captured and displayed to show server hardware availability.
Remote Control	Redirect the server video console and use your computer disk drive or disk image as a drive on the server	From the Remote Control page, you can start the Remote Control function. Using the Remote Control function, you can redirect the server console to your computer, and you can mount one of your computer disk drives, such as the CD-ROM drive or the diskette drive, on the server. When you have redirected the server console, you can use your mouse and keyboard to control the server. When you have mounted a disk, you can use it to restart the server and to update firmware on the server. You can use the Remote Console function to access the mounted disk, which will appear as a Universal Serial Bus (USB) disk drive that is attached to the server.
Serial Redirect[1]	Configure serial-to-serial redirection or serial-to-Telnet redirection.	From the Serial Redirect page, you can use the serial redirection quick setup to simplify the configuration of serial-to-serial redirection or serial-to-Telnet redirection.
PXE Network Boot	Change the host server startup (boot) sequence for the next restart to attempt a PXE/DHCP network startup.	If your server BIOS and Preboot Execution Environment (PXE) boot agent utility are properly defined, from the PXE Network Boot page you can change the host server startup (boot) sequence for the next restart to attempt a PXE/DHCP network startup. The host startup sequence will be altered only if the host is not under Privileged Access Protection (PAP). After the next restart occurs, the check box on the PXE Network Boot page will be cleared.
Firmware Update	Update firmware on the Remote Supervisor Adapter II	Use the options on the Firmware Update page to update firmware of the Remote Supervisor Adapter II.

Table 1. Remote Supervisor Adapter II actions (continued)

Link	Action	Description
Access Remote ASM[2]	Access other service processors on the ASM interconnect network	From the Access Remote ASM page, you can view a list of service processors that are present on the ASM interconnect network and establish a connection to any of those systems. **Note:** *Service processors* are Remote Supervisor Adapter IIs, Remote Supervisor Adapters, ASM processors, ASM PCI adapters, and integrated system management processors (ISMPs).
System Settings	View and change the Remote Supervisor Adapter II system settings	You can configure the server location and general information, such as the name of the Remote Supervisor Adapter II, the operating system that supports the Remote Supervisor Adapter II (Windows or Linux), server timeout settings, and contact information for the Remote Supervisor Adapter II, from the System Settings page.
	Set the Remote Supervisor Adapter II clock	You can set the Remote Supervisor Adapter II clock that is used for time stamping the entries in the event log.
Login Profiles	Configure the Remote Supervisor Adapter II login profiles and global login settings	You can define 12 login profiles that enable access to the Remote Supervisor Adapter II. You can also define global login settings that apply to all login profiles, including enabling Lightweight Directory Access Protocol (LDAP) server authentication and customizing the account security level.
Alerts	Configure remote alerts and remote alert recipients	You can configure the Remote Supervisor Adapter II to generate and forward alerts for a number of different events. On the Alerts page, you can configure the alerts that are monitored and the recipients that are notified.
	Configure local events	You can set the local events that are monitored by the Remote Supervisor Adapter II, for which notifications are sent to the IBM Director console.
	Configure alert settings	You can establish global settings that apply to all remote alert recipients, such as the number of alert retries and the delay between the retries.
Serial Port	Configure the Remote Supervisor Adapter II serial ports[1] and modem settings[2]	From the Serial Port page, you can configure the serial ports[1] and modem settings[2] that are used by the Remote Supervisor Adapter II. You can also configure the serial redirect and command-line interface (CLI) settings.[1]
Port assignments	Change the port numbers of the Remote Supervisor Adapter II protocols.	From the Port Assignments page, you can change the port numbers of Remote Supervisor Adapter II protocols (for example, HTTP, HTTPS, Telnet, and SNMP).
Network Interfaces	Configure the network interfaces of the Remote Supervisor Adapter II	From the Network Interfaces page, you can configure network-access settings for the Ethernet connection on the Remote Supervisor Adapter II. The Remote Supervisor Adapter II Ethernet connection enables remote access using a Web browser. You can also configure the point-to-point protocol (PPP) access through the Remote Supervisor Adapter II serial port.
Network Protocols	Configure the network protocols of the Remote Supervisor Adapter II	You can configure Simple Network Management Protocol (SNMP), Domain Name System (DNS), and Simple Mail Transfer Protocol (SMTP) settings that are used by the Remote Supervisor Adapter II from the Network Protocols page. You can also configure LDAP parameters.

Table 1. Remote Supervisor Adapter II actions (continued)

Link	Action	Description
Security	Configure the Secure Sockets Layer (SSL)	You can enable or disable SSL and manage the SSL certificates that are used. You can also enable or disable whether an SSL connection is used to connect to an LDAP server.
Configuration File	Back up and restore the Remote Supervisor Adapter II configuration	You can back up, modify, and restore the configuration of the Remote Supervisor Adapter II, and view a configuration summary, from the Configuration File page.
Restore Defaults	Restore the Remote Supervisor Adapter II defaults	**Attention:** When you click **Restore Defaults**, all of the modifications you made to the Remote Supervisor Adapter II are lost. You can reset the configuration of the Remote Supervisor Adapter II to the factory defaults.
Restart ASM	Restart the Remote Supervisor Adapter II	You can restart the Remote Supervisor Adapter II.
Log off	Log off the Remote Supervisor Adapter II	You can log off your connection to the Remote Supervisor Adapter II.

[1] This feature is available for the Remote Supervisor Adapter II SlimLine, except when the SlimLine is installed in any of the following servers:

- IBM xSeries 236
- IBM xSeries 260
- IBM xSeries 336
- IBM xSeries 346
- IBM xSeries 366
- IBM xSeries 460
- IBM System x3800
- IBM System x3850
- IBM System x3950

[2] This feature is not available for the Remote Supervisor Adapter II SlimLine.

You can click the **View Configuration Summary** link, which is available on most pages, to quickly view the configuration of the Remote Supervisor Adapter II.

Chapter 3. Configuring the Remote Supervisor Adapter II

Use the links under **ASM Control** in the navigation pane to configure the Remote Supervisor Adapter II.

- From the System Settings page, you can:
  - Set system information
  - Select the operating system to support (Microsoft Windows or Linux)

    Important: For the Remote Supervisor Adapter II to function correctly, the specified operating system must match the operating system of the server in which the Remote Supervisor Adapter II is installed.
    - Select **Linux** before installing Remote Supervisor Adapter II software for Linux operating systems.
    - Select **Other** before installing Remote Supervisor Adapter II software for Microsoft Windows and Novell Netware operating systems.
  - Set server timeouts
  - Set ASM date and time
- From the Login Profiles page, you can:
  - Set login profiles to control access to the Remote Supervisor Adapter II
  - Configure global login settings, such as the lockout period after unsuccessful login attempts
  - Configure the account security level
- From the Alerts page, you can:
  - Set integrated system management processor (ISMP) alert forwarding
  - Configure remote alert recipients
  - Set the number of remote alert attempts
  - Select the delay between alerts
  - Select which alerts will be sent and how they will be forwarded
- From the Serial Port page, you can:
  - Configure the serial ports of the Remote Supervisor Adapter II
  - Configure advanced modem settings (not available for the Remote Supervisor Adapter II SlimLine)
  - Set up serial redirection

  Note: Setting up serial redirection is not available for the Remote Supervisor Adapter II SlimLine in some server models.
- From the Port Assignments page, you can change the port numbers of Remote Supervisor Adapter II services.
- From the Network Interfaces page, you can:
  - Set up the Ethernet connection for the Remote Supervisor Adapter II
  - Set up a PPP over serial port connection (not available for the Remote Supervisor Adapter II SlimLine)
- From the Network Protocols page, you can:
  - Configure SNMP setup
  - Configure DNS setup
  - Telnet protocol
  - Configure SMTP setup
  - Configure LDAP setup

- – TCP command mode protocol
- – Service location protocol

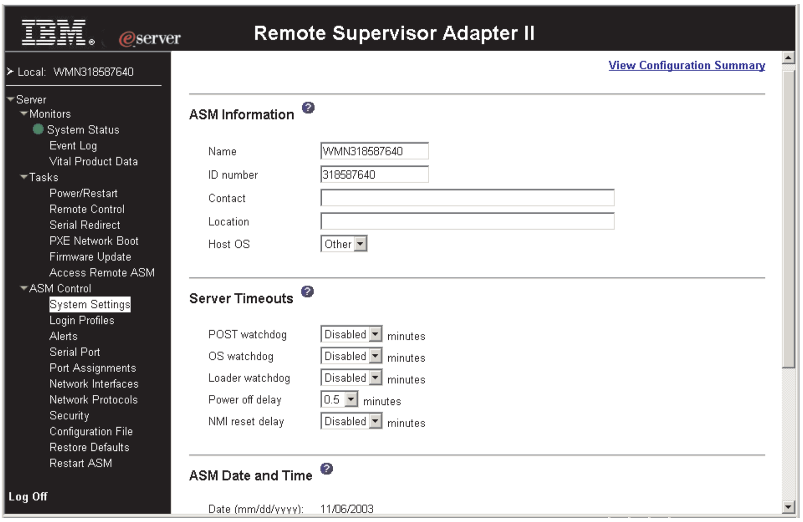
- From the Security page, you can install and configure the Secure Sockets Layer (SSL) settings.
- From the Configuration File page, you can back up, modify, and restore the configuration of the Remote Supervisor Adapter II.
- From the Restore Defaults page, you can reset the Remote Supervisor Adapter II configuration to the factory defaults.
- From the Restart ASM page, you can restart the Remote Supervisor Adapter II.

Setting system information

To set the Remote Supervisor Adapter II system information, complete the following steps:

1. Log in to the Remote Supervisor Adapter II where you want to set the system information. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **System Settings**. A page similar to the one in the following illustration is displayed.

   Note: The available fields in the System Settings page are determined by the accessed remote server.



Remote Supervisor Adapter II

ASM Information

Name: WMN318587640
ID number: 318587640
Contact:
Location:
Host OS: Other

Server Timeouts

POST watchdog: Disabled minutes
OS watchdog: Disabled minutes
Loader watchdog: Disabled minutes
Power off delay: 0.5 minutes
NMI reset delay: Disabled minutes

ASM Date and Time

Date (mm/dd/yyyy): 11/06/2003

3. In the **Name** field in the ASM Information area, type the name of the Remote Supervisor Adapter II.

   Use the **Name** field to specify a name for the Remote Supervisor Adapter II in this server. The name is included with e-mail, SNMP, and alphanumeric pager alert notifications to identify the source of the alert.

   Notes:

   a. If you plan to set up an SMTP server for e-mail alert notifications, make sure that the name in the **Name** field is valid as part of an e-mail address (for example, there are no spaces).

   b. Your Remote Supervisor Adapter II name (in the **Name** field) and the IP host name of the Remote Supervisor Adapter II (in the **Host Name** field on the Network Interfaces page) do not automatically share the same name because the **ASM Name** field is limited to 15 characters. The **Host Name** field can contain up to 63 characters. To minimize confusion, set the **ASM Name** field to the nonqualified portion of the IP host name. The nonqualified IP host name consists of up to the first period of a fully qualified IP host name. For example, for the fully qualified IP host name asmcard1.us.company.com, the nonqualified IP host name is asmcard1. For information about your host name, see “Configuring an Ethernet connection to the Remote Supervisor Adapter II” on page 39.

4. In the **ID number** field, assign the Remote Supervisor Adapter II a unique identification number.
5. In the **Contact** field, type the contact information. For example, you can specify the name and phone number of the person to contact if there is a problem with this server. You can type a maximum of 47 characters in this field.
6. In the **Location** field, type the location of the server. Include in this field sufficient detail to quickly locate the server for maintenance or other purposes. You can type a maximum of 47 characters in this field.
7. In the **HOST O/S** menu, click the type of operating system that is running on the server.

   Important: For the Remote Supervisor Adapter II to function correctly, the specified operating system must match the operating system of the server in which the Remote Supervisor Adapter II is installed.

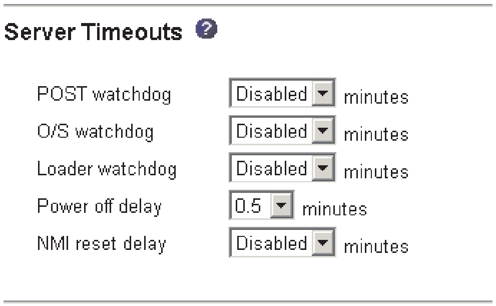
   - Select **Linux** before installing Remote Supervisor Adapter II software for Linux operating systems.
   - Select **Other** before installing Remote Supervisor Adapter II software for Microsoft Windows and Novell Netware operating systems.
8. Scroll to the bottom of the page and click **Save**.

Setting server timeouts

To set your server timeout values, complete the following steps:

1. Log in to the Remote Supervisor Adapter II where you want to set the server timeouts. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **System Settings** and scroll down to the Server Timeouts area.

   A page similar to the one in the following illustration is displayed.



Server Timeouts

POST watchdog	Disabled	minutes
O/S watchdog	Disabled	minutes
Loader watchdog	Disabled	minutes
Power off delay	0.5	minutes
NMI reset delay	Disabled	minutes

   You can set the Remote Supervisor Adapter II to respond automatically to the following events:

   - Halted power-on self-test
   - Halted operating system
   - Failure to load operating system
   - Power-off delay to shut down operating system

- Nonmaskable interrupt

3. Enable the server timeouts that correspond to the events that you want the Remote Supervisor Adapter II to respond to automatically.

POST watchdog

Use the **POST watchdog** field to specify the number of minutes that the Remote Supervisor Adapter II will wait for the server to complete a power-on self-test (POST). If the server that is being monitored fails to complete a POST within the specified time, the Remote Supervisor Adapter II generates a POST timeout alert and automatically restarts the server. The POST watchdog is then automatically disabled until the operating system is shut down and the server is power cycled (or until the operating system starts and the software is successfully loaded).

Note: Power cycling means that the server is turned off and then immediately turned on.

To set the POST timeout value, select a number from the menu. To turn off this option, select **Disabled**.

Note: If the **POST Time-out** check box is selected in the Remote Alerts area of the Remote Alerts page, the Remote Supervisor Adapter II attempts to forward the alert to all configured remote alert recipients. Also, the POST watchdog requires a specially constructed POST routine that is available only on specific IBM servers. If this routine does not exist on your server, all settings in this field are ignored.

For more information about POST routines, see the documentation that comes with your server.

O/S watchdog

Use the **O/S watchdog** field to specify the number of minutes between checks of the operating system by the Remote Supervisor Adapter II. If the operating system fails to respond to one of these checks, the Remote Supervisor Adapter II generates an O/S timeout alert and restarts the server. After the server is restarted, the O/S watchdog is disabled until the operating system is shut down and the server is power cycled.

To set the O/S watchdog value, select a time interval from the menu. To turn off this watchdog, select **Disabled**. To capture operating-system-failure screens, you must enable the watchdog in the **O/S watchdog** field and select the **O/S Time-out** check box in the Remote Alerts area of the Alerts page.

Notes:

a. The O/S watchdog feature requires that the Remote Supervisor Adapter II software be installed on the server. For information about installing this software, see the *Remote Supervisor Adapter II Installation Guide*.
b. If the **O/S Time-out** check box is selected in the Remote Alerts area of the Alerts page, the Remote Supervisor Adapter II will attempt to send an alert to all configured remote alert recipients.

Loader watchdog

Use the **Loader watchdog** field to specify the number of minutes that the Remote Supervisor Adapter II waits between the completion of

POST and the starting of the operating system. If this interval is exceeded, the Remote Supervisor Adapter II generates a loader timeout alert and automatically restarts the server. After the server is restarted, the loader timeout is automatically disabled until the operating system is shut down and the server is power cycled (or until the operating system starts and the software is successfully loaded).

To set the loader timeout value, select the time limit that the Remote Supervisor Adapter II will wait for the operating-system startup to be completed. To turn off this watchdog, select **Disabled**.

Notes:

a. Before you start (boot) an operating system that does not have the Remote Supervisor Adapter II software installed (this can also include using a flash update diskette), make sure to select **Disabled** in the **Loader watchdog** field to prevent an unwanted restart of your server.

b. If the **Loader Time-out** check box is selected in the Remote Alerts area of the Alerts page, the Remote Supervisor Adapter II will send an alert to all configured remote alert recipients.

Power off delay

Attention: Read the following information to prevent the loss of data or damage to data when you perform a remote shutdown of your operating system:

> If the Windows 2000, Windows Server 2003, Red Hat Linux, SUSE Linux, or Novell NetWare operating system is installed on your server, you have to install only the Remote Supervisor Adapter II software to support remote operating-system shutdown.
>
> **Note:** If the value in the **Power off delay** field is less than 45 seconds, the Remote Supervisor Adapter II software will adjust the value to 45 seconds when it is loaded. You can decrease the power-off delay value after the server has started, but the Remote Supervisor Adapter II software will reset it to 45 seconds on the next server restart. The Remote Supervisor Adapter II software will not change a power-off delay value that is 45 seconds or greater.

Use the **Power off delay** field to specify the number of minutes that the Remote Supervisor Adapter II will wait for the operating system to shut down before turning off the server.

Shut down your server to determine how long it takes to shut down. Add a time buffer to that value and use it as your power-off delay setting to ensure that the operating system has time for an orderly shutdown before power is removed from the server.

To set the power-off delay value, select the time from the menu.

NMI reset delay

Use the **NMI reset delay** field to specify the length of time, in minutes, that the Remote Supervisor Adapter II waits to automatically restart the server after a nonmaskable interrupt (NMI) is triggered. A nonmaskable interrupt usually indicates a critical error such as a hardware fault. A nonmaskable interrupt usually signals a parity error in the memory subsystem.

To disable the automatic server restart after a nonmaskable interrupt, select **Disabled**.

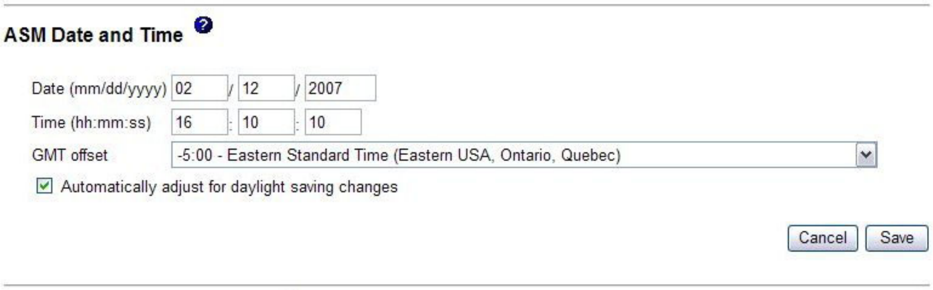
4. Scroll to the bottom of the page and click **Save**.

Setting the date and time

The Remote Supervisor Adapter II contains its own real-time clock to time stamp all events that are logged in the event log. Alerts that are sent by e-mail, LAN, and SNMP use the real-time clock setting to time stamp the alerts. The clock settings support Greenwich mean time (GMT) offsets and daylight saving time (DST) for added ease-of-use for administrators who are managing systems remotely over different time zones. You can remotely access the event log even if the server is turned off or disabled.This facilitates immediate problem determination and resolution.

To verify the date and time settings of the Remote Supervisor Adapter II, complete the following steps:

1. Log in to the Remote Supervisor Adapter II where you want to set the ASM date and time values. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **System Settings** and scroll down to the **ASM Date and Time** area, which shows the date and time when the Web page was generated.
3. To override the date and time settings and to enable daylight saving time (DST) and Greenwich mean time (GMT), click **Set ASM Date and Time**. A page similar to the one in the following illustration is displayed.



ASM Date and Time

Date (mm/dd/yyyy) 02 / 12 / 2007

Time (hh:mm:ss) 16 : 10 : 10

GMT offset -5:00 - Eastern Standard Time (Eastern USA, Ontario, Quebec)

☑ Automatically adjust for daylight saving changes

4. In the **Date** field, type the numbers of the current month, day, and year.
5. In the **Time** field, type the numbers that correspond to the current hour, minutes, and seconds in the applicable entry fields. The hour (hh) must be a number from 00 to 23 as represented on a 24-hour clock. The minutes (mm) and seconds (ss) must be numbers from 00 to 59.
6. In the **GMT offset** field, type the number that specifies the offset, in hours, from Greenwich mean time (GMT), corresponding to the time zone where the server is located.
7. Select or clear the **Automatically adjust for daylight saving changes** check box to specify whether the Remote Supervisor Adapter II clock will automatically adjust when the local time changes between standard time and daylight saving time.
8. Click **Save**.

Synchronizing clocks in a network

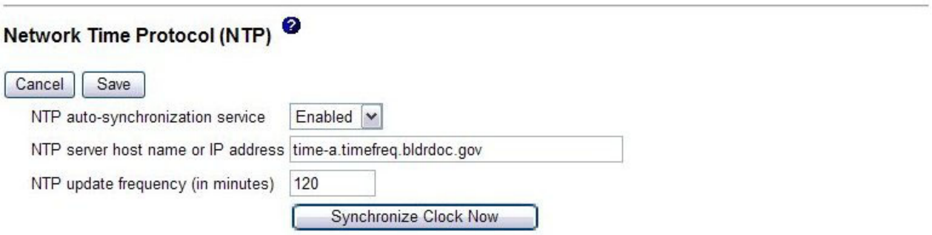
The Network Time Protocol (NTP) provides a way to synchronize clocks throughout a computer network, enabling any NTP client to obtain the correct time from an NTP server.

The Remote Supervisor Adapter II NTP feature provides a way to synchronize the Remote Supervisor Adapter II real-time clock with the time that is provided by an NTP server. You can specify the NTP server that is to be used, specify the frequency with which the Remote Supervisor Adapter II will be synchronized, enable or disable the NTP feature, and request an immediate time synchronization.

The NTP feature does not provide the extended security and authentication that are provided through encryption algorithms in NTP Version 3 and NTP Version 4. The Remote Supervisor Adapter II NTP feature supports only the Simple Network Time Protocol (SNTP) without authentication.

To set up the Remote Supervisor Adapter II NTP feature settings, complete the following steps:

1. Log in to the Remote Supervisor Adapter II on which you want to synchronize the clocks in the network. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **System Settings** and scroll down to the **Network Time Protocol (NTP)** area. A page similar to the one in the following illustration is displayed.



Network Time Protocol (NTP)

NTP auto-synchronization service: Enabled

NTP server host name or IP address: time-a.timefreq.bldrdoc.gov

NTP update frequency (in minutes): 120

3. You can select from the following setttings:

   NTP auto-synchronization service
   Use this selection to enable or disable automatic synchronization of the ASM clock with an NTP server.

   NTP server host name or IP address
   Use this field to specify the name of the NTP server to be used for clock synchronization.

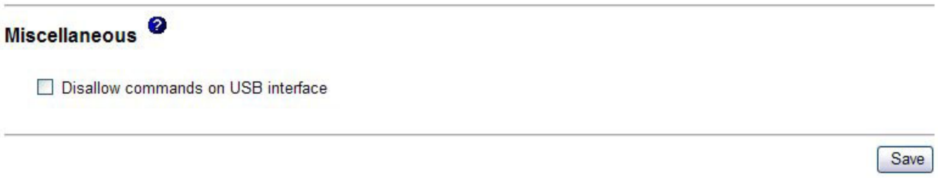
   NTP update frequency
   Use this field to specify the approximate interval (in minutes) between synchronization requests.

   Synchronize Clock Now
   Click this button to request an immediate synchronization instead of waiting for the interval time to lapse.
4. Click **Save**.

Disabling the USB device driver interface

If you want to prevent any application that is running on the server from requesting the Remote Supervisor Adapter II to perform tasks, you must disable the USB device driver interface. To disable the USB device driver interface, complete the following steps.

1. Log in to the Remote Supervisor Adapter II on which you want to disable the USB device driver interface. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **System Settings** and scroll down to the **Miscellaneous** area. A page similar to the one in the following illustration is displayed.



Miscellaneous

☐ Disallow commands on USB interface

3. Select the **Disallow commands on USB interface** check box to disable the USB device driver interface. Selecting this option does not affect the USB remote control functions (for example, keyboard, mouse, and mass storage). When you disable the USB device driver interface, the in-band system-management applications such as the management processor command-line interface (MPCLI) and Advanced Settings Utility (ASU) are disabled. If you try to use system-management applications while the device driver interface is disabled, there might be unwanted consequences.
4. Click **Save**.

Important: If you disable the USB device driver interface, you cannot perform an in-band update of the Remote Supervisor Adapter II firmware using the Linux or Windows flash utilities. If the USB device driver interface is disabled, use the Firmware Update option on the Remote Supervisor Adapter II Web interface to update the firmware. For more information, see “Updating firmware” on page 88.

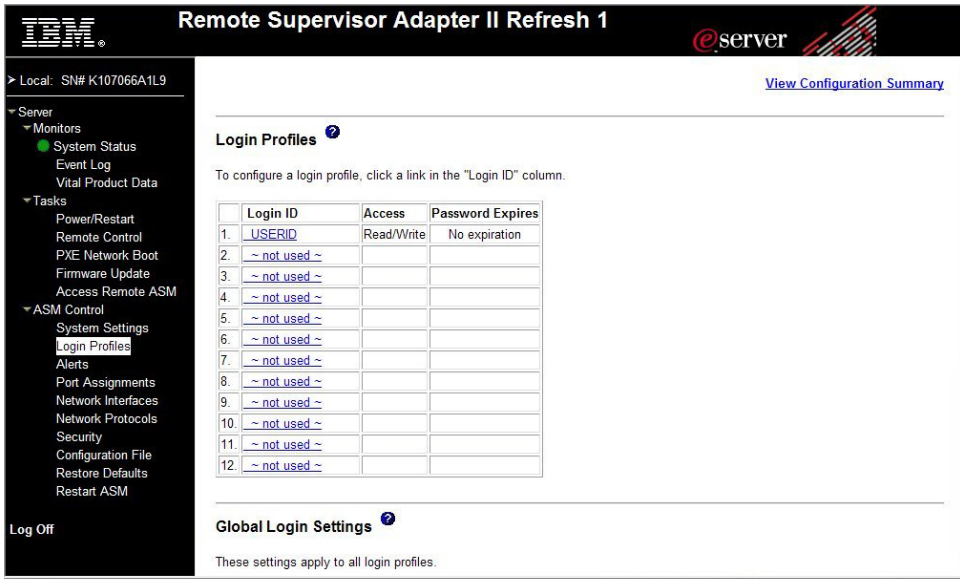
To enable the USB device driver interface after it has been disabled, clear the **Disallow commands on USB interface** check box and then restart the server so that the USB device driver is loaded and initialized correctly.

Creating a login profile

Use the Login Profiles table to view, configure, or change individual login profiles. Use the links in the Login ID column to configure individual login profiles. You can define up to 12 unique profiles. Each link in the Login ID column is labeled with the configured login ID for that particular profile. If you have not configured a profile, the name of the link, by default, will be `~ not used ~`.

To configure a login profile, complete the following steps:

1. Log in to the Remote Supervisor Adapter II where you want to create a login profile. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Login Profiles**. The Login Profiles page displays each login ID, the login access level, and the password expiration information, as shown in the following illustration.



Login Profiles

To configure a login profile, click a link in the "Login ID" column.

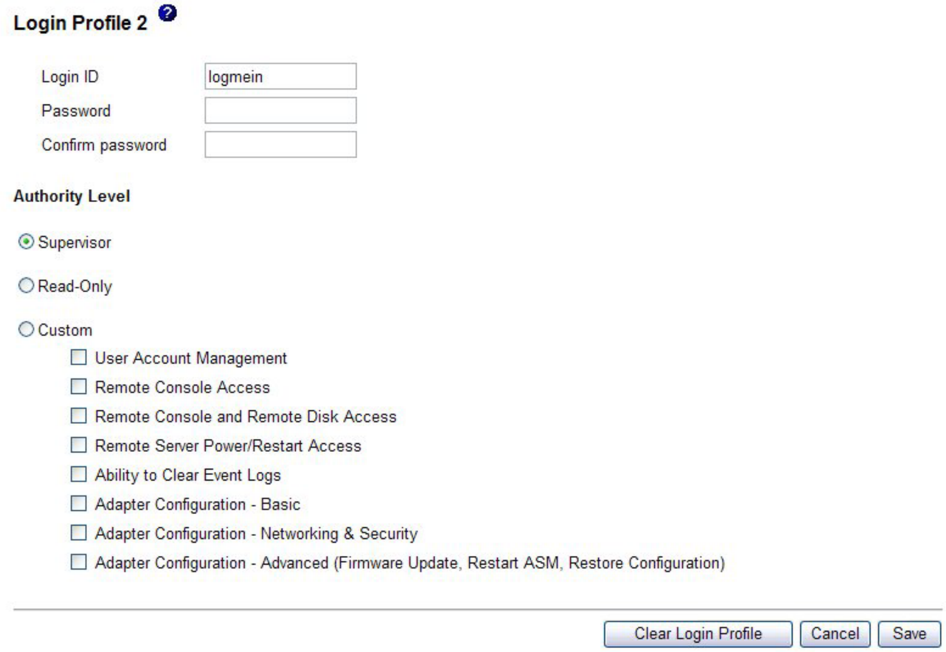
	Login ID	Access	Password Expires
1.	USERID	Read/Write	No expiration
2.	~ not used ~		
3.	~ not used ~		
4.	~ not used ~		
5.	~ not used ~		
6.	~ not used ~		
7.	~ not used ~		
8.	~ not used ~		
9.	~ not used ~		
10.	~ not used ~		
11.	~ not used ~		
12.	~ not used ~		

Global Login Settings

These settings apply to all login profiles.

Note: By default, the Remote Supervisor Adapter II is configured with one login profile that enables remote access using a login user ID of `USERID` and a password of `PASSW0RD` (the 0 is a zero, not the letter O). To avoid a potential security exposure, change this default login profile during the initial setup of the Remote Supervisor Adapter II.

3. Click one of the unused login profile links. An individual profile page similar to the one in the following illustration is displayed.



Login Profile 2

Login ID	logmein
Password	
Confirm password	

Authority Level

● Supervisor

○ Read-Only

○ Custom

- □ User Account Management
- □ Remote Console Access
- □ Remote Console and Remote Disk Access
- □ Remote Server Power/Restart Access
- □ Ability to Clear Event Logs
- □ Adapter Configuration - Basic
- □ Adapter Configuration - Networking & Security
- □ Adapter Configuration - Advanced (Firmware Update, Restart ASM, Restore Configuration)

4. In the **Login ID** field, type the name of the profile.

   You can type a maximum of 15 characters in the **Login ID** field. Valid characters are uppercase and lowercase letters, numbers, periods, and underscores.

Note: This login ID is used to grant remote access to the Remote Supervisor Adapter II.

5. In the **Password** field, assign a password to the login ID.

   A password must contain at least five characters, one of which must be a nonalphabetic character. Null or empty passwords are accepted.

   Note: This password is used with the login ID to grant remote access to the Remote Supervisor Adapter II.
6. In the **Confirm Password** field, type the password again.
7. In the **Authority level** area, select one of the following options to set the access rights for this login ID:

   Supervisor
   The user has no restrictions.

   Read Only
   The user has read-only access only and cannot perform actions such as file transfers, power and restart actions, or remote control functions.

   Custom
   If you select the Custom option, you must select one or more of the following custom authority levels:

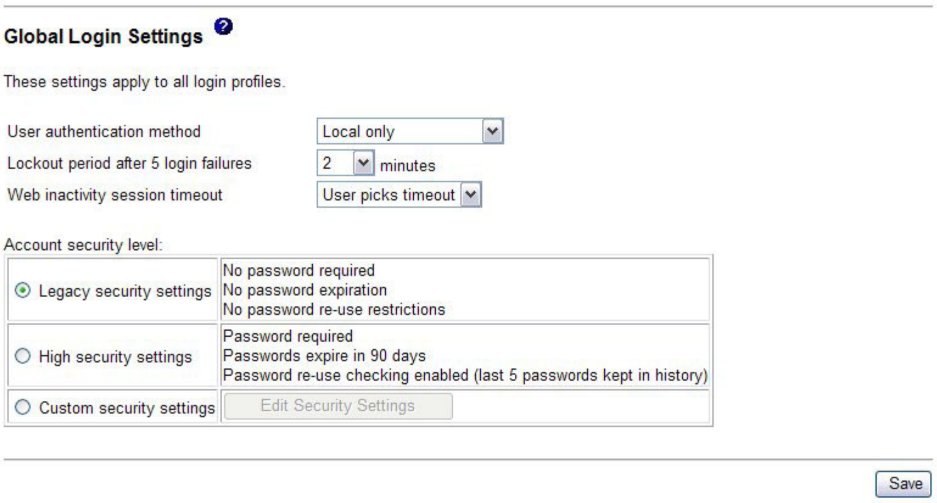
   - **User Account Management:** A user can add, modify, or delete users and change the global login settings in the Login Profiles page.
   - **Remote Console Access:** A user can access the remote console.
   - **Remote Console and Virtual Media Access:** A user can access both the remote console and the virtual media feature.
   - **Remote Server Power/Restart Access:** A user can access the power on and restart functions for the remote server. These functions are available in the Power/Restart page.
   - **Ability to Clear Event Logs:** A user can clear the event logs. Everyone can look at the event logs, but this particular permission is required to clear the logs.
   - **Adapter Configuration - Basic:** A user can modify configuration parameters in the System Settings and Alerts pages.
   - **Adapter Configuration - Networking & Security:** A user can modify configuration parameters in the Security, Network Protocols, Network Interface, Port Assignments, and Serial Port pages.
   - **Adapter Configuration (Advanced):** A user has no restrictions when configuring the adapter. In addition, the user is said to have administrative access to the Remote Supervisor Adapter II, meaning that the user can also perform the following advanced functions: firmware updates, PXE network boot, restore adapter factory defaults, modify and restore adapter configuration from a configuration file, and restart and reset the adapter.

   Note: To return the login profile to the factory defaults, click **Clear Login Profiles**.
8. Click **Save** to save your login ID settings.

Configuring the global login settings

Complete the following steps to set conditions that apply to all login profiles for the Remote Supervisor Adapter II:

1. Log in to the Remote Supervisor Adapter II for which you want to set the global login settings. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Login Profiles**.
3. Scroll down to the Global Login Settings area. A page similar to the one in the following illustration is displayed.



Global Login Settings

These settings apply to all login profiles.

User authentication method: Local only

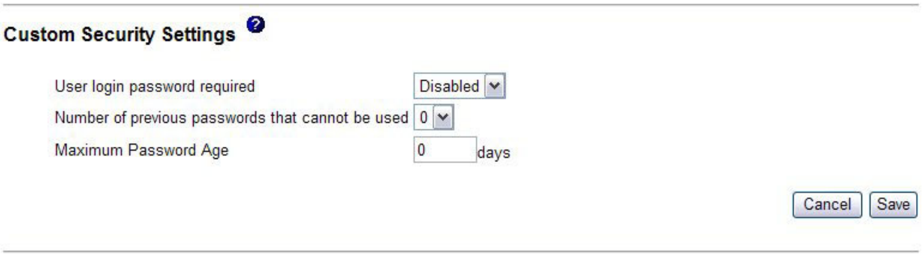
Lockout period after 5 login failures: 2 minutes

Web inactivity session timeout: User picks timeout

Account security level:

● Legacy security settings	No password required No password expiration No password re-use restrictions
○ High security settings	Password required Passwords expire in 90 days Password re-use checking enabled (last 5 passwords kept in history)
○ Custom security settings	Edit Security Settings

4. In the **User authentication method** field, specify how users who are attempting to log in are authenticated. Select one of the following authentication methods:
   - **Local only:** Users are authenticated by a search of a table that is local to the Remote Supervisor Adapter II. If there is no match on the user ID and password, access is denied. Users who are successfully authenticated are assigned the authority level that is configured in “Creating a login profile” on page 18.
   - **LDAP only:** The Remote Supervisor Adapter II attempts to authenticate the user by using the LDAP server. Local user tables on the Remote Supervisor Adapter II are never searched with this authentication method.
   - **Local first, then LDAP:** Local authentication is attempted first. If local authentication fails, LDAP authentication is attempted.
   - **LDAP first, then Local:** LDAP authentication is attempted first. If LDAP authentication fails, local authentication is attempted.
5. In the **Lockout period after 5 login failures** field, specify how long, in minutes, the Remote Supervisor Adapter II will prohibit remote login attempts, if more than five sequential failures to log in remotely are detected.
6. In the **Web inactivity session timeout** field, specify how long, in minutes, the Remote Supervisor Adapter II will wait before disconnecting an inactive Web session. Select **No timeout** to disable this feature. Select **User picks timeout** if the user will select the timeout period during the login process.
7. (Optional) In the **Account security level** area, select a password security level. The **Legacy security settings** and **High security settings** set the default values as indicated in the requirement list.
8. To customize the security setting, select **Custom security settings** and then click **Edit Security Settings**. A page similar to the one in the following illustration is displayed.



Custom Security Settings

User login password required: Disabled

Number of previous passwords that cannot be used: 0

Maximum Password Age: 0 days

You can view and change the account security management configuration on the Custom Security Settings page. When you change the **User login password required** setting, you must also have a password, to be consistent with the requirement.

User login password required
Use this field to indicate whether a login ID with no password is allowed.

Number of previous passwords that cannot be used
Use this field to indicate the number of previous passwords that cannot be reused. Up to five previous passwords can be compared. Select **0** to allow the reuse of all previous passwords.

Maximum Password Age
Use this field to indicate the maximum password age that is allowed before the password must be changed. Values of 0 to 365 days are supported. Select **0** to disable the password expiration checking.

9. Click **Save**.

Configuring remote alert settings

Note: For the Remote Supervisor Adapter II SlimLine, the configuring remote alert settings feature is available only when using LAN-based alert functionality.

You can configure remote alert recipients, the number of alert attempts, incidents that trigger remote alerts, and local alerts from the **Alerts** link on the navigation pane.

After you configure a remote alert recipient, the Remote Supervisor Adapter II will send an alert to that recipient. The alert is sent through a serial connection or a network connection, a numeric pager, or an alphanumeric pager when any event selected from the Monitored Alerts group occurs. This alert contains information about the nature of the event, the time and date of the event, and the name of the system that generated the alert.

The Remote Supervisor Adapter II offers alert redundancy for several managed systems at the same location. It sends alerts only once per connection type, even when there is more than one active LAN or serial connection. However, if one connection device fails, all other interconnected devices route the alerts to the next available connection.

Notes:

1. If the **SNMP Agent** or **SNMP Traps** fields are not set to **Enabled**, no SNMP traps are sent. For information about these fields, see “Configuring SNMP” on page 43.

2. You cannot distinguish between the alerts that are sent to remote alert recipients. All configured recipients receive each alert that you select.

Configuring remote alert recipients

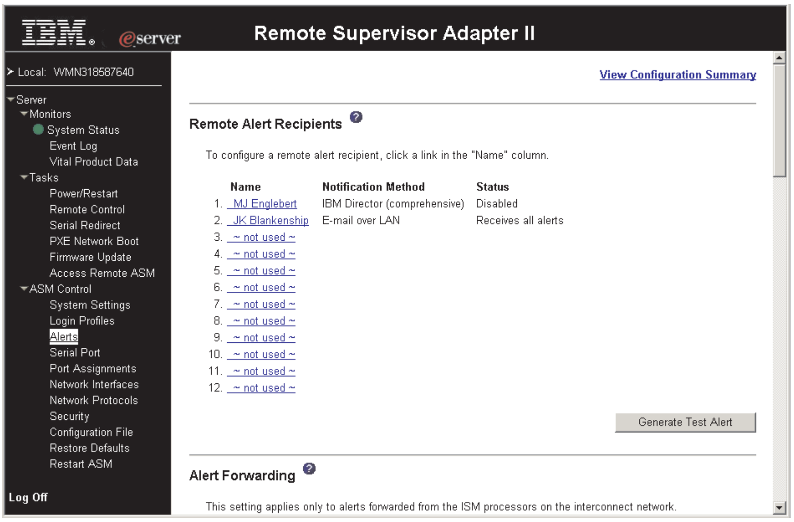
Notes:

1. For the Remote Supervisor Adapter II SlimLine, the configuring remote alert recipients feature is available only when using LAN-based alert functionality.
2. For the Remote Supervisor Adapter II SlimLine, the PPP settings are not available.

You can define up to 12 unique remote alert recipients. Each link for an alert recipient is labeled with the recipient name, notification method, and alert status.

To configure a remote alert recipient, complete the following steps:

1. Log in to the Remote Supervisor Adapter II for which you want to configure remote alert settings. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Alerts**. The Remote Alert Recipients page is displayed. You can see the notification method and alert status for each recipient, if they are set.



Remote Alert Recipients

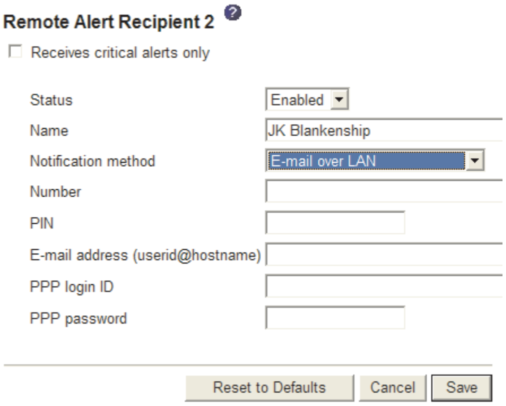
To configure a remote alert recipient, click a link in the "Name" column.

	Name	Notification Method	Status
1.	MJ Englebert	IBM Director (comprehensive)	Disabled
2.	JK Blankenship	E-mail over LAN	Receives all alerts
3.	~ not used ~		
4.	~ not used ~		
5.	~ not used ~		
6.	~ not used ~		
7.	~ not used ~		
8.	~ not used ~		
9.	~ not used ~		
10.	~ not used ~		
11.	~ not used ~		
12.	~ not used ~		

Alert Forwarding

This setting applies only to alerts forwarded from the ISM processors on the interconnect network.

3. Click one of the remote alert recipient links. An individual recipient window similar to the one in the following illustration opens.



Remote Alert Recipient 2

□ Receives critical alerts only

Status	Enabled
Name	JK Blankenship
Notification method	E-mail over LAN
Number	
PIN	
E-mail address (userid@hostname)	
PPP login ID	
PPP password	

4. To have only critical alerts sent to the recipient, select the **Receives critical alerts only** check box.
5. In the **Status** field, click **Enabled** to activate the remote alert recipient.
6. In the **Name** field, type the name of the recipient or other identifier. The name that you type appears as the link for the recipient on the Alerts page.
7. In the **Notification method** field, select the notification method for reaching the recipient. Select one of the following notification methods. Not all methods are available on all servers.
   - Numeric pager (not available for the Remote Supervisor Adapter II SlimLine)
   - Alphanumeric pager (not available for the Remote Supervisor Adapter II SlimLine)
   - IBM Director Comprehensive
   - IBM Director over Modem (not available for the Remote Supervisor Adapter II SlimLine)
   - IBM Director over LAN
   - SNMP over LAN
   - E-mail over LAN

   Note: For you to configure a remote alert recipient for IBM Director Comprehensive, IBM Director over Modem, or IBM Director over LAN, the remote alert recipient must be a server on which IBM Director Server is installed.
8. In the **Number** field, type either the phone number, IP address, or host name at which to contact the recipient.

   Type a phone number if you are using one of the following notification methods:
   - Numeric pager (follow the phone number with a comma and the personal identification number [PIN])
   - Alphanumeric pager
   - IBM Director over Modem

   Type an IP address or host name if you are using the IBM Director over LAN method.
9. Enter additional information for the selected notification method:
   - If you selected the alphanumeric pager notification method, in the **PIN** field, enter the PIN.
   - If you selected the E-mail over LAN notification method, in the **E-Mail address** field, type the e-mail address of the recipient.

     Note: For the E-mail over LAN notification method to work correctly, configure the Simple Mail Transfer Protocol (SMTP) options on the Network Protocols page. For more information about SMTP options, see “Configuring SMTP” on page 45.
10. In the **PPP login ID** field, specify the login ID or user ID that you need to log in to your Internet Service Provider (ISP).

    Note: The **PPP login ID** field is required for E-mail over PPP and SNMP over PPP notification methods. For remote access on a Windows operating system, this is usually the user ID of the account that is set up.

For example, to log in to the IBM Global Network®, the PPP login ID is in the following format: secureip.*y.z* where *y* is your account name and *z* is your user ID.

11. In the **PPP password** field, type the password that is used to log in to the ISP.

    This field is required only for E-mail over PPP and SNMP over PPP notification methods.
12. Click **Save** to save your remote alert recipient profile. Repeat step 2 on page 23 through step 24 for each remote alert recipient profile.
13. Click **Generate Test Alert** on the Remote Alert Recipients page to send a test alert to all configured remote alert recipients.

Note: All selected alert events are sent to all configured remote alert recipients.

Forwarding alerts

Note: For the Remote Supervisor Adapter II SlimLine, the forwarding alerts feature is not available.

The Alert Forwarding setting applies only to alerts that are forwarded from integrated system management processors (ISMPs) on an ASM interconnect network. The ISMPs on the network forward alerts only to the Remote Supervisor Adapter or Remote Supervisor Adapter II that is designated as the gateway. The gateway adapter then forwards the alerts through an Ethernet connection on the network to the alert recipients. A Remote Supervisor Adapter II is a gateway to the interconnect network if one of the following circumstances is true:

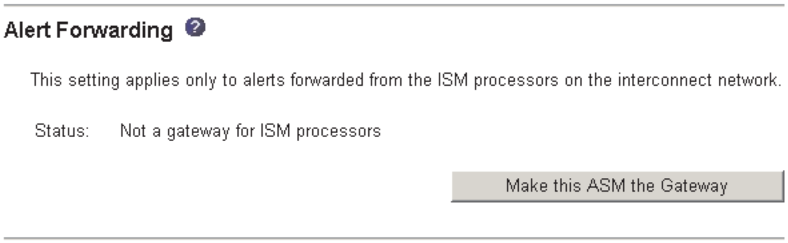
- On the Alerts Forwarding page, you click **Make this ASM the Gateway**.
- The Remote Supervisor Adapters and Remote Supervisor Adapter IIs on the network negotiate and designate the adapter to be the gateway. This occurs if you do not configure one of the Remote Supervisor Adapters or Remote Supervisor Adapter IIs on the network to be the gateway.

Notes:

1. There must be at least one Remote Supervisor Adapter or Remote Supervisor Adapter II on the interconnect network for ISMP alerts to be forwarded. At any time, only one Remote Supervisor Adapter or Remote Supervisor Adapter II can be the gateway on an interconnect network.
2. When Remote Supervisor Adapters and Remote Supervisor Adapter IIs are on the interconnect network, a Remote Supervisor Adapter II should be configured as the gateway.
3. When a user configures a Remote Supervisor Adapter or Remote Supervisor Adapter II to be the gateway, any existing gateway (user-defined or negotiated) ceases to be the gateway.
4. The remote alert recipients and monitored alerts for the ISMPs on the interconnect network must be configured on the gateway Remote Supervisor Adapter or Remote Supervisor Adapter II; otherwise, the alerts will not be forwarded.
5. In the event of a gateway adapter failure, a new gateway is automatically negotiated. To enable alerts to be forwarded by the negotiated gateway, you must also configure the remote alert recipients and monitored alerts on Remote Supervisor Adapters and Remote Supervisor Adapter IIs that are potential gateways.

To verify whether the selected Remote Supervisor Adapter II is the gateway to the interconnect network, complete the following steps:

1. Log in to the Remote Supervisor Adapter II for which you want to see the alert forwarding status. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Alerts** and scroll down to the **Alert Forwarding** area.



Alert Forwarding

This setting applies only to alerts forwarded from the ISM processors on the interconnect network.

Status: Not a gateway for ISM processors

3. The **Status** field shows whether the Remote Supervisor Adapter II is the gateway and, if it is, whether it is a user-configured or negotiated gateway. The following values are possible:
   - Not a gateway for ISMPs
   - User configured gateway for ISMPs
   - Negotiated gateway for ISMPs

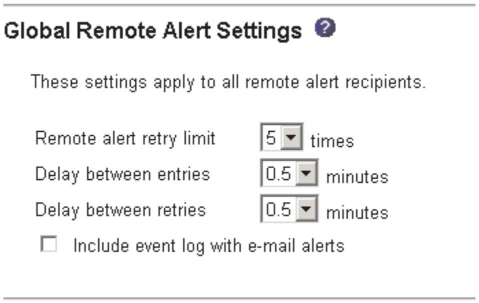
Setting remote alert attempts

Note: For the Remote Supervisor Adapter II SlimLine, the configuring remote alert attempts feature is available only when using LAN-based alert functionality.

The remote alert attempts settings apply only to forwarded alerts.

Complete the following steps to set the number of times that the Remote Supervisor Adapter II attempts to send an alert:

1. Log in to the Remote Supervisor Adapter II on which you want to set remote alert attempts. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Alerts** and scroll down to the Global Remote Alert Settings area.



Global Remote Alert Settings

These settings apply to all remote alert recipients.

Remote alert retry limit 5 times

Delay between entries 0.5 minutes

Delay between retries 0.5 minutes

□ Include event log with e-mail alerts

Use these settings to define the number of remote alert attempts and the length of time between the attempts. The settings apply to all configured remote alert recipients.

Remote alert retry limit

Use the **Remote alert retry limit** field to specify the number of additional times that the Remote Supervisor Adapter II will attempt to send an alert to a recipient.

Delay between entries

Use the **Delay between entries** field to specify the time interval (in minutes) that the Remote Supervisor Adapter II will wait before sending an alert to the next recipient in the list.

Delay between retries

Use the **Delay between retries** field to specify the time interval (in minutes) that the Remote Supervisor Adapter II will wait between retries to send an alert to a recipient.

3. Select the **Include event log with e-mail alerts** check box to attach the local event log to all e-mail alert notifications. The event log provides a summary of the most recent events and assists with problem identification and fast recovery.

   Notes:

   a. To send the event log as an e-mail attachment, you must select E-mail over LAN as the notification method for at least one remote alert recipient.
   b. Event logs that are attached in an e-mail are not forwarded to a Remote Supervisor Adapter or Remote Supervisor Adapter II on the ASM interconnect network.
4. Scroll to the bottom of the page and click **Save**.

Setting remote alerts

Note: For the Remote Supervisor Adapter II SlimLine, the setting remote alerts feature is available only when using LAN-based alert functionality.

To select the remote alerts that are to be sent, complete the following steps:

1. Log in to the Remote Supervisor Adapter II where you want to set remote alerts. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Alerts** and scroll down to the **Monitored Alerts** area.
3. Select the events that you want the Remote Supervisor Adapter II to monitor.

   The remote alerts are categorized by the following levels of severity:

   - Critical
   - Warning
   - System

   All alerts are stored in the event log and sent to all configured remote alert recipients.

   Critical alerts

   Critical alerts are generated for events that signal that the server is no longer functioning. If the **Select all critical alerts** check box is selected, an alert can be sent for any critical alert.

Table 2. Critical remote alerts

Alphanumeric pager code	Alphanumeric recovery code	Event	Action
00	50	Temperature irregularity	Generates an alert if any of the monitored temperatures are outside critical threshold values. To view the threshold values, click the temperature readings on the System Health page. If a critical temperature condition is detected, the server shuts down and turns off, regardless of the alert notification setting.
01	51	Voltage irregularity	Generates an alert if the voltages of any of the monitored power supplies fall outside their specified operational ranges. To view the operational ranges, click the voltage readings on the System Health page. If a critical voltage condition is detected, the server shuts down and turns off, regardless of the alert notification setting.
02	52	Tampering	Generates an alert if physical intrusion of the server is detected. Tamper monitoring is not available on some servers, in which case this setting is ignored.
03	53	Multiple fan failure	Generates an alert if two or more of the cooling fans in the server fail.
04	54	Power failure	Generates an alert if any of the server power supplies fail.
05	55	Hard disk drive failure	Generates an alert if one or more of the hard disk drives in the server fail.
06	56	VRM failure	Generates an alert if one or more voltage regulator modules (VRMs) fail. This setting is ignored for servers without VRMs.
07-09			Reserved for future use.

Warning alerts

Warning alerts are generated for events that might progress to a critical level. If the **Select all warning alerts** check box is selected, an alert can be sent for any warning alert.

Table 3. Warning remote alerts

Alphanumeric pager code	Alphanumeric recovery code	Event	Action
10	60	Redundant power supply failure	Generates an alert if a redundant power supply fails.
11	61	Single fan failure	Generates an alert if one fan fails.
12	62	Temperature irregularity	Generates an alert if any monitored temperatures are outside the warning threshold values. To access these temperature threshold values, click the temperature readings on the System Health page. Unlike the critical temperature event, this event will not initiate a server shutdown.
13	63	Voltage irregularity	Generates an alert if any monitored voltages are outside the warning threshold values. To access these voltage range values, click the voltage readings on the System Health page. Unlike the critical voltage event, this event will not initiate an automatic server shutdown.
14 - 19			Reserved for future use.

System alerts

System alerts are generated for events that occur as a result of system errors. If the **Select all system alerts** check box is selected, an alert can be sent for any system alert.

Notes:

a. The **Select all system alerts** check box is not available on all servers.

b. Hard disk drive Predictive Failure Analysis (PFA) alerts are not monitored.

Table 4. System remote alerts

Alphanumeric pager code	Alphanumeric recovery code	Event	Action
20	70	POST timeout	Generates an alert if an enabled POST timeout value is exceeded. The POST timeout value is configured in the **Server Timeouts** area on the System page.
21	71	O/S timeout	Generates an alert if an enabled operating system timeout value is exceeded. The operating system timeout value is configured in the **Server Timeouts** area on the System page. The O/S timeout alert must be checked to enable remote operating-system-failure screen capture.
22	72	Test alert	Generates an alert if the **Generate Test Alert** button is clicked on the Remote Alert Recipients page.
23	73	Power off	Generates an alert if the server is turned off.
24	74	Power on	Generates an alert if the server is turned on.
25	75	Boot failure	Generates an alert if an error occurs that prevents the server from starting.
26	76	Loader timeout	Generates an alert if an enabled server loader timeout value is exceeded. The system loader timeout value is configured in the **Server Timeouts** area on the System page.
27	77	PFA notification	Generates an alert if a PFA notification is generated by the server hardware. This feature is available only on servers that have PFA-enabled hardware.
28 - 29			Reserved for future use.
38	88	Partition configuration	Generates an alert if a partition configuration notification is generated by the server. This feature is available only on servers that have partitionable hardware.
39	89	Event log	Generates an alert if the event log reaches 75% or 100% of capacity, or if the log is cleared (Refresh 2 or later firmware only).

4. Scroll to the bottom of the page and click **Save**.

Setting local events

Note: For the Remote Supervisor Adapter II SlimLine, the setting local events feature is available only when using LAN-based alert functionality.

Complete the following steps to select the local events to which the Remote Supervisor Adapter II will respond:

1. Log in to the Remote Supervisor Adapter II where you want to set local events. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Alerts** and scroll down to the **Monitored Local Events** area.
3. Select the events that you want to store in the event log. The Remote Supervisor Adapter II stores the notification only in the event log.

   Local events are generated for events that are sent to IBM Director, if it is installed, on the server where the ASM subsystem is located. These events are not sent to remote alert recipients. If the **Select all local events** check box is selected, an alert can be sent for any local event.

Table 5. Local events

Event	Action
Event log 75% full	Generates a local notification if the event log reaches 75% of capacity.
Voltage irregularity	Generates a local notification if any of the monitored voltages exceed their thresholds.
Power off	Generates a local notification if the server is turned off.
Power supply failure	Generates a local notification if a power-supply failure is detected.
Event log full	Generates a local notification if the event log reaches its capacity. At capacity, the oldest events are deleted.
Redundant power supply failure	Generates a local notification if the redundant power supply fails.
Tampering	• Generates a local notification if the server cover is removed. This feature is available only on some servers. • Generates a local notification if there are five login failures (refresh 2 or later firmware only).
DASD failure	Generates a local notification if any hard disk drive failures are detected.
Remote login	Generates a local notification if a remote login occurs.
Temperature irregularity	Generates a local notification if any of the monitored temperatures exceed thresholds.
Fan failure	Generates a local notification if one or more cooling fans fail.
PFA notification	Generates a local notification if any of the hardware in the server generates a PFA event.
Partition configuration	Generates a local notification if any of the hardware in the server generates a partition configuration event.

4. Scroll to the bottom of the page and click **Save**.

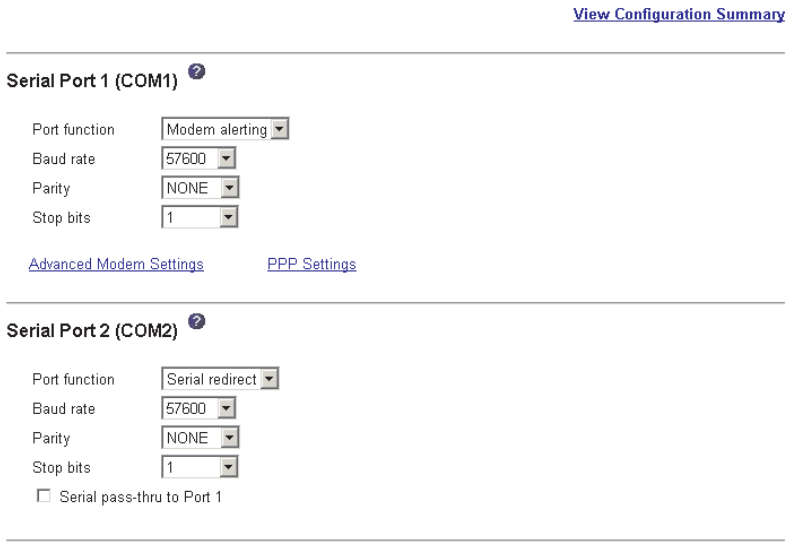
Configuring the serial connectors

Note: This feature is not available for the Remote Supervisor Adapter II SlimLine on some server models.

To configure the serial connector, complete the following steps:

1. Log in to the Remote Supervisor Adapter II on which you want to configure the serial port. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.

2. In the navigation pane, click **Serial Port**. A page similar to the one in the following illustration is displayed.



View Configuration Summary

Serial Port 1 (COM1)

Port function: Modem alerting
Baud rate: 57600
Parity: NONE
Stop bits: 1

Advanced Modem Settings   PPP Settings

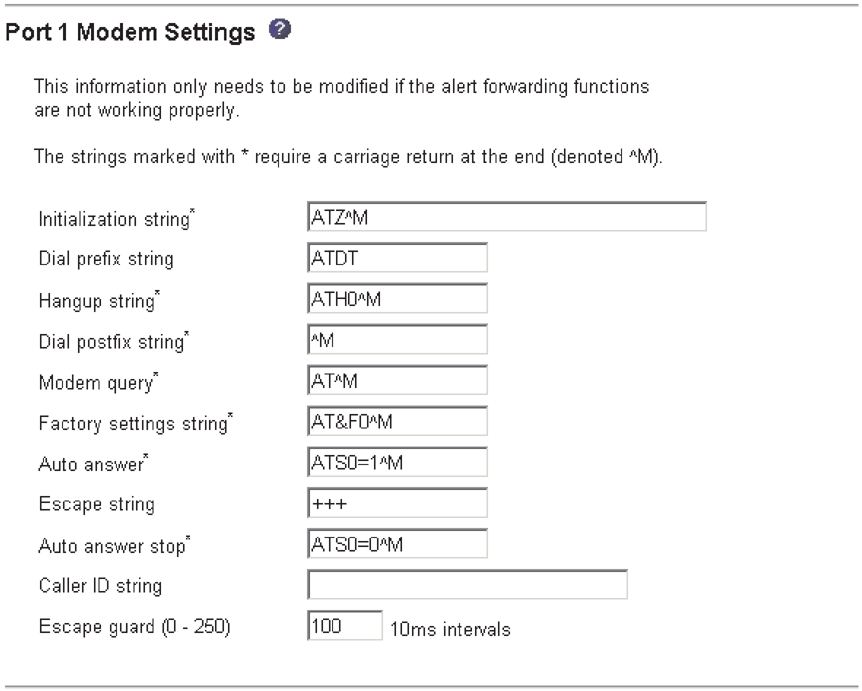
Serial Port 2 (COM2)

Port function: Serial redirect
Baud rate: 57600
Parity: NONE
Stop bits: 1
□ Serial pass-thru to Port 1

3. In the **Port function** field, select the function for which this serial port will be used. If the Remote Supervisor Adapter II supports point-to-point protocol (PPP) over a serial port, select **PPP** as the port function to enable the PPP interface for that port. Any other selection disables the PPP interface. Select **None**, if it is available, to disable the port. If you select **PPP**, click **PPP Settings** to configure the settings. For more information, see “Configuring PPP access over a serial connection” on page 42.
4. In the **Baud rate** field, select the data-transfer rate.

   Use the **Baud rate** field to specify the data-transfer rate of your serial port connection. To set the baud rate, select the data-transfer rate, in bits per second, that corresponds to your serial port connection.
5. In the **Parity** field, select the error detection that is to be used in your serial connection.
6. In the **Stop bits** field, select the number of data-terminating 1-bits that will follow the data or any parity bit to mark the end of a transmission (normally a byte or character).

   Note: The number of data bits is preset to 8 and cannot be changed.
7. Click **Save**.
8. If you need to set advanced settings, click **Advanced Modem Settings**. A page similar to the one in the following illustration is displayed.



Port 1 Modem Settings

This information only needs to be modified if the alert forwarding functions are not working properly.

The strings marked with * require a carriage return at the end (denoted ^M).

Initialization string*	ATZ^M
Dial prefix string	ATDT
Hangup string*	ATH0^M
Dial postfix string*	^M
Modem query*	AT^M
Factory settings string*	AT&F0^M
Auto answer*	ATS0=1^M
Escape string	+++
Auto answer stop*	ATS0=0^M
Caller ID string	
Escape guard (0 - 250)	100 10ms intervals

Set these values only if the alert forwarding functions are not working properly. Each string that is marked with an asterisk (*) must have a carriage return (^M) manually entered at the end of the field value.

The following table describes the initialization strings for this modem.

Table 6. Port 1 settings

Field	What you type
Initialization string*	Type the initialization string that will be used for the specified modem. A default string is provided (ATE0). Do not change this string unless your dial-out functions are not working properly.
Dial prefix string	Type the initialization string that is used before the number that is to be dialed. The default is ATDT.
Hangup string*	Type the initialization string that will be used to instruct the modem to disconnect. A default string is provided (ATH0). Do not change this string unless your dial-out functions are not working properly.
Dial postfix string*	Type the initialization string that is used after the number is dialed to tell the modem to stop dialing. The default is ^M.
Modem query*	Type the initialization string that is used to find out whether the modem is attached. The default is AT.
Factory settings string*	Type the initialization string that returns the modem to its factory settings when the modem is initialized. The default is AT&F0.
Auto answer*	Type the initialization string that is used to tell the modem to answer the phone when it rings. The default is to answer after one ring, ATS0=1.
Escape string	Type the initialization string that returns the modem to command mode when it is currently communicating with another modem. The default is +++.
Auto answer stop*	Type the initialization string that is used to tell the modem to stop answering the phone automatically when it rings. The default is ATS0=0.
Caller ID string	Type the initialization string that will be used to get caller ID information from the modem.

Table 6. Port 1 settings (continued)

Field	What you type
Escape guard (0 - 250)	Type the length of idle time that is used before and after the escape string is issued to the modem, so that the modem will recognize the escape string. This value is measured in 10-millisecond intervals. The default value is 1 second.

9. Click **Save**.

If you need to provide a new initialization string, see the documentation that came with your modem. Your initialization string must contain commands that configure your modem as follows:

- Command echoing OFF
- Online character echoing OFF
- Result codes ENABLED
- Verbal result codes ENABLED
- All codes and connect messages with BUSY and DT detection
- Protocol identifiers added — LAPM/MNP/NONE V42bis/MNP5
- Normal CD operations
- DTR ON-OFF hang-up, disable AA and return to command mode
- CTS hardware flow control
- RTS control of receive data to computer
- Queued and nondestructive break, no escape state

Note: The abbreviations in these commands have the following meanings:

AA	auto answer
CD	carrier detect
CTS	clear to send
DT	data transfer
DTR	data terminal ready
LAPM	link access protocol for modems
MNP	microcom networking protocol
RTS	ready to send

Configuring the dual serial connectors for serial redirection

Note: This feature is not available for the Remote Supervisor Adapter II SlimLine on some server models.

You can use the ASM breakout cable with dual serial connectors to connect the server serial port (using a null modem cable) to a client workstation that uses a terminal-emulation program such as Hilgraeve HyperTerminal or to a hardware terminal server (also using a null modem cable). The Remote Supervisor Adapter II acts as a pass-through device. Using this single serial connection to a terminal server or client workstation, a system administrator can access the serial features of both the operating system and the Remote Supervisor Adapter II. The Remote Supervisor Adapter II command-line interface (CLI) provides text-based power control and server reset ability.

To use the ASM breakout cable with dual serial connectors for a single serial connection to a terminal server, make sure that:

- Your server basic input/output system (BIOS) supports the single serial connection. This BIOS serial support is needed to provide power-on self-test (POST), setup, and end-to-end remote access.

- You update the Remote Supervisor Adapter II firmware. For information about obtaining Remote Supervisor Adapter II firmware and software, see the *Installation Guide*.
- Your operating system has serial support for text management in the operating system. The following operating systems have serial support:
  - Microsoft Windows Server 2003 Enterprise Edition with emergency management services for serial console support
  - Linux operating systems with Agetty serial console support

Serial-to-serial redirection

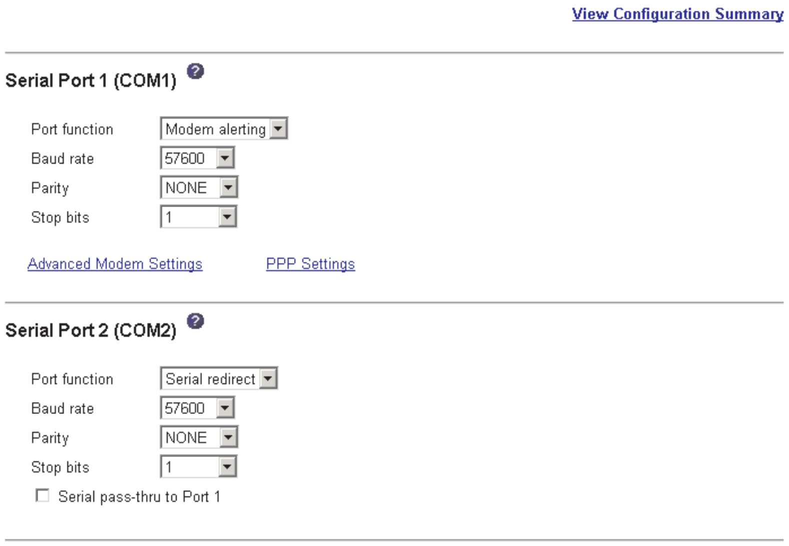
Serial-to-serial redirection enables the Remote Supervisor Adapter II to pass data between COM1 and COM2. This mode is useful when a single serial connection is required to a client computer or a hardware terminal server.

When serial authentication is enabled, the serial command-line interface session is authenticated through the local logon profiles or through an LDAP server.

For serial redirection quick setup information, see “Serial redirection quick setup” on page 86.

To set up the software configuration for serial-to-serial redirection configuration, complete the following steps:

1. Log in to the Remote Supervisor Adapter II on which you want to configure the serial port. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Serial Port**. A page similar to the one in the following illustration is displayed.



View Configuration Summary

Serial Port 1 (COM1)

Port function: Modem alerting
Baud rate: 57600
Parity: NONE
Stop bits: 1

Advanced Modem Settings   PPP Settings

Serial Port 2 (COM2)

Port function: Serial redirect
Baud rate: 57600
Parity: NONE
Stop bits: 1
☐ Serial pass-thru to Port 1

3. In the **Serial Port 1** area, set the following values for the fields:
   a. In the **Port function** field, select **Serial redirect**.

      Note: The serial ports are enabled independently for serial redirection. For serial-to-serial redirection, both ports must be set to **Serial redirect**. The available options for COM1 are Modem alerting, PPP, and Serial redirect. If COM2 is enabled, it supports only serial redirection.

b. Configure the **Baud rate**, **Parity**, and **Stop bits** fields to match the serial port settings on the server.

   Notes:

   1) Serial redirection does not support hardware-based flow control. Disable the terminal flow control.
   2) To prevent buffer overrun and character loss, configure both serial ports with the same baud rate. The Remote Supervisor Adapter II provides a 512-character buffer on both incoming and outgoing serial streams.

4. In the **Serial Port 2** area, set the following values for the fields:
   a. In the **Port function** field, select **Serial redirect**.
   b. Configure the **Baud rate**, **Parity**, and **Stop bits** fields to match the serial port settings on the server.

      Note: Serial redirection does not support hardware-based flow control. Disable the terminal flow control.
5. Select the **Serial pass-thru to Port 1** check box to force the link between COM1 and COM2. Both ports must be active and in serial redirection mode to enable this function. If the function is not enabled, the command-line interface must be invoked, and the console command must be used to link the appropriate ports together.

Serial-to-Telnet redirection

Serial-to-Telnet redirection enables a system administrator to use the Remote Supervisor Adapter II as a serial terminal server. Either one or both serial ports can be accessed from a Telnet connection when serial redirection is enabled.

For serial redirection quick setup information, see “Serial redirection quick setup” on page 86.

The Remote Supervisor Adapter II uses the custom command-line interface enter key sequence to return from a serial redirection session. The command-line interface enter key sequence defaults to the Microsoft Windows Server 2003 emergency management services compatible key sequence: Press the Escape key, then the open parenthesis symbol [( ].

Notes:

1. The Remote Supervisor Adapter II allows two open Telnet sessions. The Telnet sessions can independently access the serial ports so that multiple users can have a concurrent view of a redirected serial port.
2. One serial port must be enabled for serial redirection to enable the **console** command.
3. Telnet does not use the command-line interface exit key sequence. The command-line interface **console** command must be used to select a COM port.
4. The Telnet session is authenticated through the local logon profiles or through an LDAP server.

Example session

```
telnet 192.168.70.125 (Press Enter.)
Connecting to 192.168.70.125...
username: USERID (Press Enter.)
password: ******** (Press Enter.)
SN# J1RAE32S000> console 1 (Press Enter.)
unsupported console
SN# J1RAE32S000> console 2 (Press Enter.)
```

Note: All traffic from COM2 is now routed to the Telnet session. All traffic from the Telnet session is routed to COM2.

```
ESC (
```

Note: In the default mode (EMS compatible), press Esc then the open parenthesis symbol [( ] to return to the command-line interface.

```
SN# J1RAE32S000> exit (Press Enter.)
```

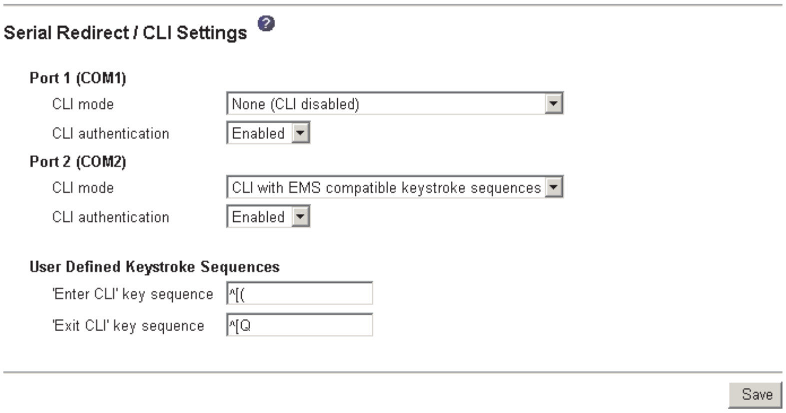
Configuring the command-line interface settings

The Remote Supervisor Adapter II command-line interface provides a set of commands that you can use for power control, monitoring and configuring the Remote Supervisor Adapter II and the server. The command-line interface is available from either or both serial ports and from up to two simultaneous Telnet sessions.

The Remote Supervisor Adapter II command-line interface commands and their descriptions are listed in Chapter 6, "Command-line interface," on page 91.

To use the command-line interface, complete the following steps:

1. Log in to the Remote Supervisor Adapter II on which you want to configure the serial port. For more information, see Chapter 2, "Opening and using the Web interface," on page 5.
2. In the navigation pane, click **Serial Port**.
3. Scroll to the **Serial Redirect Settings / CLI Settings** area.



Serial Redirect / CLI Settings

Port 1 (COM1)
CLI mode: None (CLI disabled)
CLI authentication: Enabled

Port 2 (COM2)
CLI mode: CLI with EMS compatible keystroke sequences
CLI authentication: Enabled

User Defined Keystroke Sequences
'Enter CLI' key sequence: ^[(
'Exit CLI' key sequence: ^[Q

4. Use the following information to select the values for the fields.

   CLI mode

   Use the command-line interface mode options to configure whether the command-line interface is available from a serial port and whether a custom key sequence must be used to enter and exit. The default setting enables the Remote Supervisor Adapter II to function in Microsoft Windows Server 2003-compatible environments.

   Select from the following values:

   - **None (CLI disabled)**

     The Remote Supervisor Adapter II does not allow access to the command-line interface from this serial port.

   - **CLI with EMS compatibility keystroke sequences**

     The Remote Supervisor Adapter II accepts three key sequences when in Emergency Management Services-compatible mode. The sequences are defined by the Microsoft Windows Server 2003 Emergency Management Services specification. The key sequences that are supported are described in the following table.

Table 7. Supported Emergency Management Services key sequences

Task	Key sequence
Enter the Remote Supervisor Adapter II command-line interface	Press Esc (The Remote Supervisor Adapter II sends Esc * as an acknowledgment to the command.
Exit the command-line interface	Press Esc Q
Reset the server	Press Esc R Esc r Esc R No authentication is required to reset the server in this mode.

- **CLI with user defined keystroke sequences**

  The Remote Supervisor Adapter II accepts the enter and exit sequences that are defined in the Enter CLI key sequence and Exit CLI key sequence. The fields are defined in the following sections. The Remote Supervisor Adapter II does not provide a server reset key sequence in this mode.

CLI authentication

The command-line interface can be automatically invoked when a user types the Enter CLI key sequence. This mode is provided for environments where the serial port is secured outside the Remote Supervisor Adapter II. Telnet sessions always require the user to authenticate.

Select from the following values:

- **Enabled**

  A user name/password prompt is presented. Authentication is required to get access to the command-line interface commands.
- **Disabled**

  No user name/password is presented when the key sequence to enter the command-line interface is pressed. The serial port has full access to all available commands.

User Defined Keystroke Sequences

The enter key sequence specifies the key sequence that the Remote Supervisor Adapter II will require to begin a command-line interface session. The exit key sequence specifies the key sequence that is required to exit from the command-line interface.

When you select **CLI with user defined keystroke sequences** for the serial port, the serial port (COM1 and COM2) sessions use the custom command-line interface enter and exit key sequences.

The Telnet sessions always use the custom command-line interface enter key sequence to return to the Remote Supervisor Adapter II command-line interface.

The sequences can be up to 19 characters. Use the caret symbol (^) to specify control characters in the Web interface.

The default sequences are equivalent to the EMS key sequences. When **CLI with user defined keystroke sequence** is selected, the

EMS reset key sequence is not available, and the Remote Supervisor Adapter II will not issue the EMS acknowledgment when the enter key sequence is accepted.

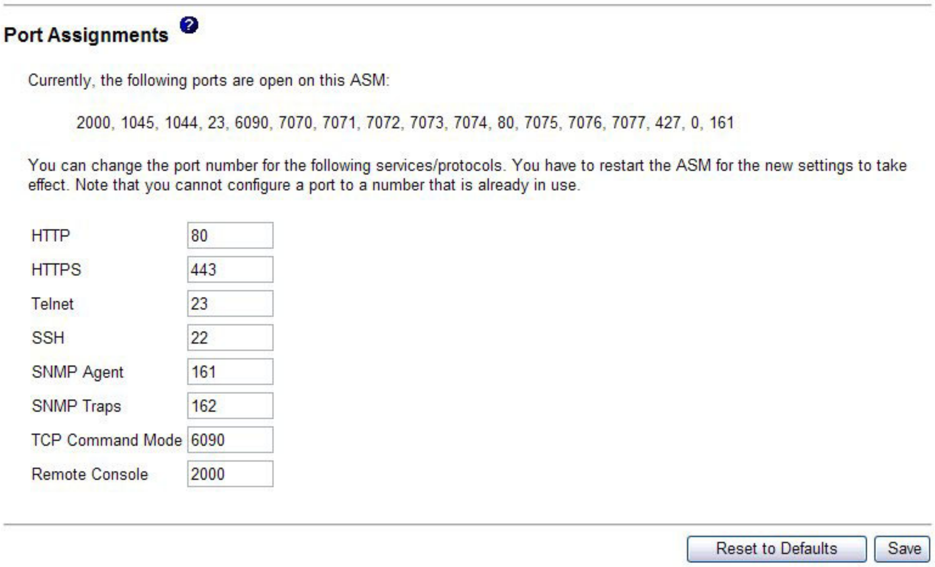
5. At the bottom of the page, click **Save**.
6. To begin using the new settings, in the left navigation pane, click **Restart ASM**.

To set up the hardware connections, see the *Installation Guide*.

Configuring port assignments

To change the port numbers of Remote Supervisor Adapter II services, complete the following steps:

1. Log in to the Remote Supervisor Adapter II where you want to configure the port assignments. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Port Assignments**. A page similar to the one in the following illustration is displayed.



Port Assignments

Currently, the following ports are open on this ASM:

2000, 1045, 1044, 23, 6090, 7070, 7071, 7072, 7073, 7074, 80, 7075, 7076, 7077, 427, 0, 161

You can change the port number for the following services/protocols. You have to restart the ASM for the new settings to take effect. Note that you cannot configure a port to a number that is already in use.

HTTP	80
HTTPS	443
Telnet	23
SSH	22
SNMP Agent	161
SNMP Traps	162
TCP Command Mode	6090
Remote Console	2000

3. Use the following information to assign values for the fields:

HTTP This is the port number for the HTTP server of the Remote Supervisor Adapter II. The default port number is 80. Other valid values are in the range 1 through 65535. If you change this port number, you must add this port number, preceded by a colon, at the end of the Web address. For example, if the HTTP port is changed to 8500, type `http://hostname:8500/` to open the Remote Supervisor Adapter II Web interface. Note that you must type the prefix `http://` before the IP address and port number.

HTTPS
This is the port number that is used for Web interface HTTPS (SSL) traffic. The default value is 443. Other valid values are in the range 1 through 65535.

Telnet This is the port number for the Telnet server of the Remote Supervisor Adapter II. The default value is 23. Other valid values are in the range 1 through 65535.

SSH This is the port for the SSH. The default is 22.

SNMP Agent
This is the port number for the SNMP agent that runs on the Remote Supervisor Adapter II. The default value is 161. Other valid values are in the range 1 through 65535.

SNMP Traps
This is the port number that is used for SNMP traps. The default value is 162. Other valid values are in the range 1 through 65535.

TCP command mode
This is the port that IBM Director uses for out-of-band communication with the Remote Supervisor Adapter II. The default is 6090.

Remote Console
This is the port that the remote control function uses to view and interact with the server console. The default is 2000.

The following port numbers are reserved and can be used only for the corresponding services.

Table 8. Reserved port numbers

Port number	Services used for
1044	Remote disk
1045	Remote disk on card
427	SLP
7070 through 7073 (for xSeries 445 Type 8870 only)	Partition management
7070 through 7077 (for xSeries 460 Type 8872 only)	Partition management

4. Click **Save**.

Configuring network interfaces

On the Network Interfaces page, you can set access to the Remote Supervisor Adapter II by:

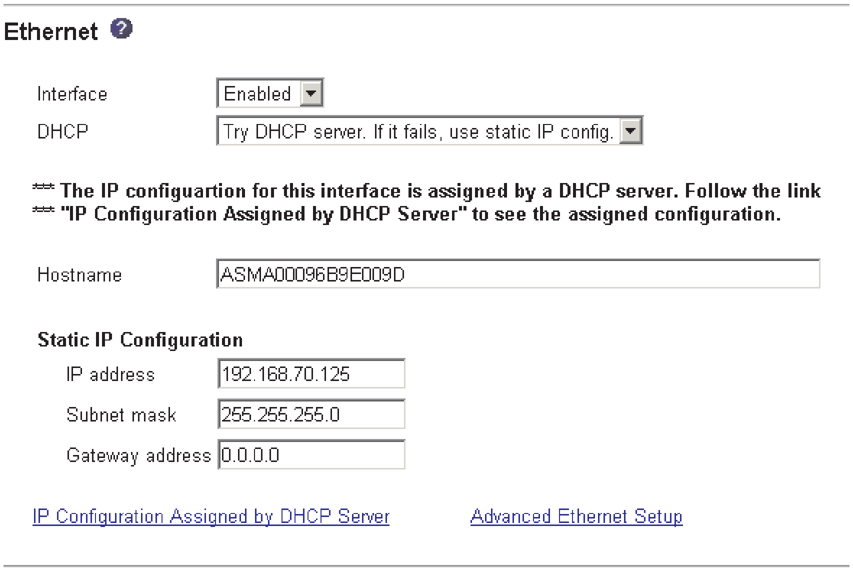
- Configuring an Ethernet connection to a Remote Supervisor Adapter II
- Configuring point-to-point protocol access over a serial connector

Configuring an Ethernet connection to the Remote Supervisor Adapter II

To configure the Ethernet setup for the Remote Supervisor Adapter II, complete the following steps:

1. Log in to the Remote Supervisor Adapter II where you want to set up the configuration. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Network Interfaces**. A page similar to the one in the following illustration is displayed.

   Note: The values in the following illustration are examples. Your settings will be different.



Ethernet

Interface: Enabled

DHCP: Try DHCP server. If it fails, use static IP config.

*** The IP configuartion for this interface is assigned by a DHCP server. Follow the link
*** "IP Configuration Assigned by DHCP Server" to see the assigned configuration.

Hostname: ASMA00096B9E009D

Static IP Configuration

IP address: 192.168.70.125

Subnet mask: 255.255.255.0

Gateway address: 0.0.0.0

IP Configuration Assigned by DHCP Server

Advanced Ethernet Setup

3. If you want to use an Ethernet connection, select **Enabled** in the **Interface** field. Ethernet is enabled by default.
4. If you want to use a Dynamic Host Configuration Protocol (DHCP) server connection, enable it by clicking either of the following choices in the DHCP field:
   - **Enabled**
   - **Try DHCP server. If it fails, use static IP config.**

   The default setting is **Try DHCP server. If it fails, use static IP config.**

   Note: Do not enable DHCP unless you have an accessible, active, and configured DHCP server on your network. When DHCP is used, the automatic configuration will override any manual settings.

   If DHCP is enabled, the host name is assigned as follows:
   - If the **Hostname** field contains an entry, the Remote Supervisor Adapter II DHCP support will request the DHCP server to use this host name.
   - If the **Hostname** field does not contain an entry, the Remote Supervisor Adapter II DHCP support will request the DHCP server to assign a unique host name to the Remote Supervisor Adapter II.

   If you enabled DHCP, go to step 12 on page 42.

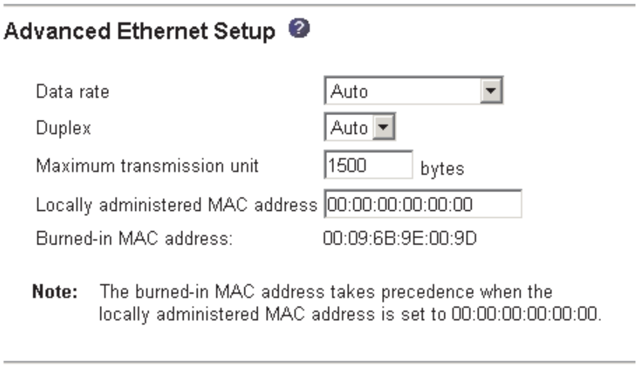
   If you have not enabled DHCP, continue with step 5.
5. Type the IP host name of the Remote Supervisor Adapter II in the **Hostname** field.

   You can enter a maximum of 63 characters in this field, which represents the IP host name of the Remote Supervisor Adapter II. The host name defaults to ASMA, followed by the Remote Supervisor Adapter II burned-in media access control (MAC) address.

   Note: The IP host name of the Remote Supervisor Adapter II (the **Hostname** field) and Remote Supervisor Adapter II name (the **ASM Name** field on the System page) do not automatically share the same name, because the **ASM Name** field is limited to 15 characters but the **Hostname** field can contain up to 63 characters. To minimize confusion, set the **ASM Name** field to the nonqualified portion of the IP host name. The nonqualified IP host name consists of up to the first period of a fully qualified IP host name. For example, for the fully qualified IP host name asmcard1.us.company.com, the nonqualified IP host name is asmcard1. For information about your host name, see “Setting system information” on page 12.

6. In the **IP address** field, type the IP address of the Remote Supervisor Adapter II. The IP address must contain four integers from 0 through 255 with no spaces and separated by periods.
7. In the **Subnet mask** field, type the subnet mask that is used by the Remote Supervisor Adapter II. The subnet mask must contain four integers from 0 through 255 with no spaces or consecutive periods and separated by periods.

   The default setting is 255.255.255.0.
8. In the **Gateway address** field, type your network gateway router. The gateway address must contain four integers from 0 through 255 with no spaces or consecutive periods and separated by periods.
9. Scroll to the bottom of the page and click **Save**.
10. Click **Advanced Ethernet Setup** if you need to set additional Ethernet settings.



Advanced Ethernet Setup

Data rate: Auto

Duplex: Auto

Maximum transmission unit: 1500 bytes

Locally administered MAC address: 00:00:00:00:00:00

Burned-in MAC address: 00:09:6B:9E:00:9D

Note: The burned-in MAC address takes precedence when the locally administered MAC address is set to 00:00:00:00:00:00.

The following table describes the functions on the Advanced Ethernet page.

Table 9. Advanced Ethernet setup

Field	**Function**
Data rate	Use the **Data Rate** field to specify the amount of data that is to be transferred per second over your LAN connection. To set the data rate, click the menu and select the data-transfer rate, in Mb[1], that corresponds to the capability of your network. To automatically detect the data-transfer rate, select **Auto**, which is the default value.
Duplex	Use the **Duplex** field to specify the type of communication channel that is used in your network. To set the duplex mode, select one of the following choices: **Full** enables data to be carried in both directions at once. **Half** enables data to be carried in either one direction or the other, but not both at the same time. To automatically detect the duplex type, select **Auto**, which is the default value.
Maximum transmission unit	Use the **Maximum transmission unit** field to specify the maximum size of a packet (in bytes) for your network interface. For Ethernet, the valid maximum transmission unit (MTU) range is 60 - 1500. The default value for this field is 1500.

Table 9. Advanced Ethernet setup (continued)

Field	Function
Burned-in MAC address	The burned-in MAC address is a unique physical address that is assigned to this Remote Supervisor Adapter II by the manufacturer. The address is also a read-only field.
Locally administered MAC address	Enter a physical address for this Remote Supervisor Adapter II in the **Locally administered MAC address** field. If a value is specified, the locally administered address overrides the burned-in MAC address. The locally administered address must be a hexadecimal value from 000000000000 through FFFFFFFFFFFF. This value must be in the form *xx*:*xx*:*xx*:*xx*:*xx*:*xx* where *x* is a number between 0 and 9. The Remote Supervisor Adapter II does not support the use of a multicast address.The first byte of a multicast address is an odd number (the least significant bit is set to 1). Therefore, the first byte must be an even number.
[1]Mb equals approximately 1 000 000 bits.	

11. Modify the advanced Ethernet settings as necessary.
12. Scroll to the bottom of the page and click **Save**.
13. Click **Back** to return to the Network Interfaces page. If DHCP is enabled, the server automatically assigns the host name, IP address, gateway address, subnet mask, domain name, DHCP server IP address, and up to three DNS server IP addresses.
14. If DHCP is enabled, to view the DHCP server assigned setting, click **IP Configuration Assigned by DHCP Server**.
15. Click **Save**.
16. In the navigation pane, click **Restart ASM** to activate the changes.

Configuring PPP access over a serial connection

Note: This feature is not available for the Remote Supervisor Adapter II SlimLine.

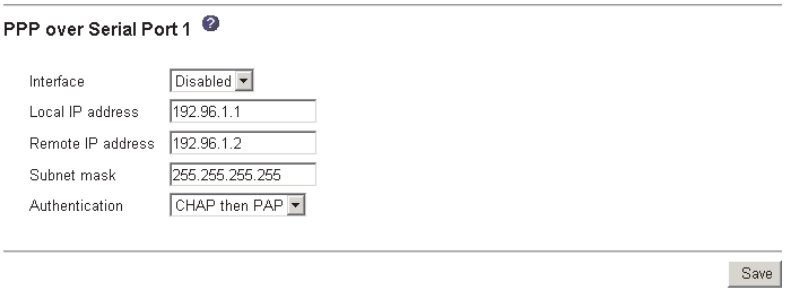
Use the point-to-point protocol (PPP) access method if you do not have Ethernet access. You can use PPP through your serial port to enable access to the Remote Supervisor Adapter II through a Telnet session or a Web browser.

Note: If you enable the PPP interface, the Remote Supervisor Adapter II cannot use the serial port for serial remote access.

To configure PPP access over a serial port, complete the following steps:

1. Log in to the Remote Supervisor Adapter where you want to configure PPP access over a serial port. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Network Interfaces**. Scroll down to the PPP over Serial Port 1 area.

   Note: The values in the following illustration are examples. Your settings will be different.



PPP over Serial Port 1

Interface	Disabled
Local IP address	192.96.1.1
Remote IP address	192.96.1.2
Subnet mask	255.255.255.255
Authentication	CHAP then PAP

3. In the **Interface** field, select **Enabled**.
4. In the **Local IP address** field, type the local IP address for the PPP interface on this Remote Supervisor Adapter II. The field defaults to 192.96.1.1. The IP address must contain four integers from 0 through 255 separated by periods and no spaces.
5. In the **Remote IP address** field, type the remote IP address that this Remote Supervisor Adapter II will assign to a remote user. The field defaults to 192.96.1.2. The remote IP address must contain four integers from 0 through 255 separated by periods and no spaces.
6. In the **Subnet mask** field, type the subnet mask for the Remote Supervisor Adapter II to use. The default is 255.255.255.255. The subnet mask must contain four integers from 0 through 255 separated by periods and no spaces.
7. In the **Authentication** field, specify the type of authentication protocol that will be negotiated when a PPP connection is attempted.
   - The **PAP Only** setting uses a two-way handshake procedure to validate the identity of the originator of the connection. The weak privileged access protection (PAP) authentication protocol is necessary if a plain text password must be available to simulate a login at a remote host.
   - The **CHAP Only** setting uses a three-way handshake procedure to validate the identity of the originator of a connection when a connection occurs at any later time. The challenge handshake authentication protocol (CHAP) is stronger than the PAP protocol and protects against playback and trial-and-error attacks.
   - The **CHAP then PAP** setting tries to authenticate using CHAP first. If the originator of the connection does not support CHAP, PAP is tried as a secondary authentication protocol. The **CHAP then PAP** setting is the default.
8. Click **Save**.
9. In the navigation pane, click **Restart ASM** to activate the changes.

Configuring network protocols

On the Network Protocols page, you can perform the following functions:

- Configure Simple Network Management Protocol (SNMP)
- Configure Domain Name System (DNS)
- Configure Simple Mail Transfer Protocol (SMTP)
- Configure Lightweight Directory Access Protocol (LDAP)

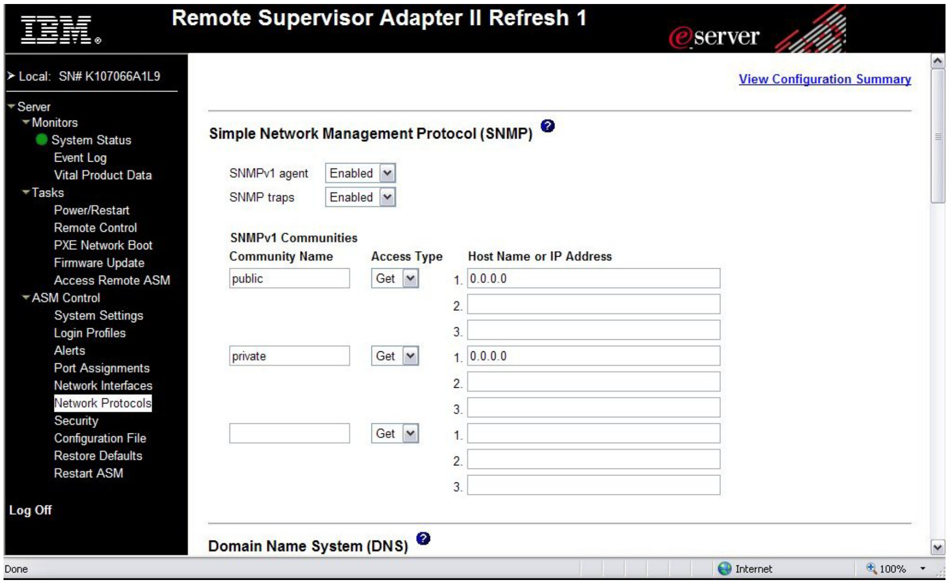
Configuring SNMP

You can query the SNMP agent to collect the sysgroup information and to send configured SNMP alerts to the configured host names or IP addresses.

Note: If you plan to configure Simple Network Management Protocol (SNMP) traps on the Remote Supervisor Adapter II, you must install and compile the management information base (MIB) on your SNMP manager. The MIB supports SNMP traps. The MIB is included in the Remote Supervisor Adapter II firmware update package that you downloaded from the IBM Support Web site.

To configure SNMP, complete the following steps:

1. Log in to the Remote Supervisor Adapter II where you want to configure SNMP. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **System Settings**. In the ASM information page that is displayed, specify system contact and system location information. For information about the System Settings page, see “Setting system information” on page 12.
3. Scroll to the bottom of the page and click **Save**.
4. In the navigation pane, click **Network Protocols**. A page similar to the one in the following illustration is displayed.



Simple Network Management Protocol (SNMP)

SNMPv1 agent: Enabled

SNMP traps: Enabled

SNMPv1 Communities

Community Name	Access Type		Host Name or IP Address
public	Get	1.	0.0.0.0
		2.	
		3.	
private	Get	1.	0.0.0.0
		2.	
		3.	
	Get	1.	
		2.	
		3.	

Domain Name System (DNS)

5. Select **Enabled** in the **SNMP agent** and **SNMP traps** fields to forward alerts to SNMP communities on your network. To enable the SNMP agent, the following criteria must be met:
   - System contacts must be specified on the System Settings page. For information about the System Settings page settings, see “Setting system information” on page 12.
   - System location must be specified on the System Settings page.
   - At least one community name must be specified.
   - At least one valid IP address or host name (if DNS is enabled) must be specified for that community.

   Note: Alert recipients whose notification method is SNMP will not receive alerts unless both the **SNMP agent** and the **SNMP traps** fields are set to **Enabled**.

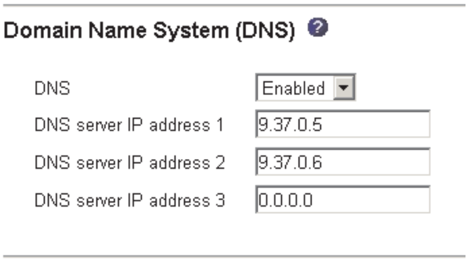
6. Set up a community to define the administrative relationship between SNMP agents and SNMP managers. You must define at least one community. Each community definition consists of the following parameters:

   - Name
   - IP address
   - Access Type (Refresh 2 or later firmware only)

   If any of these parameters is not correct, SNMP management access is not granted.

   Note: If an error message window opens, make the necessary adjustments to the fields that are listed in the error window. Then, scroll to the bottom of the page and click **Save** to save your corrected information. You must configure at least one community to enable this SNMP agent.

7. In the **Community Name** field, enter a name or authentication string to specify the community.
8. In the **Access Type** field, select an access type. Select **Trap** to allow all hosts in the community to receive traps; select **Get** to allow all hosts in the community to receive traps and query MIB objects; select **Set** to allow all hosts in the community to receive traps, query, and set MIB objects.
9. In the corresponding **Host Name** or **IP Address** field, enter the host name or IP address of each community manager.
10. If a DNS server is not available on your network, scroll to the bottom of the page and click **Save**. Otherwise, scroll to the Domain Name System (DNS) area. A page similar to the one in the following illustration is displayed.



Domain Name System (DNS)

DNS: Enabled

DNS server IP address 1: 9.37.0.5

DNS server IP address 2: 9.37.0.6

DNS server IP address 3: 0.0.0.0

11. If a DNS server (or servers) is available on your network, select **Enabled** in the **DNS** field. The **DNS** field specifies whether you use a DNS server on your network to translate host names into IP addresses.
12. If you enabled DNS, in the **DNS server IP address** fields, specify the IP addresses of up to three DNS servers on your network. Each IP address must contain integers from 0 through 255 separated by periods.
13. Scroll to the **Telnet Protocol** area. You can set the maximum number of concurrent Telnet users or disable Telnet access.
14. Scroll to the bottom of the page and click **Save**.
15. In the navigation pane, click **Restart ASM** to activate the changes.

Configuring SMTP

Complete the following steps to specify the IP address or host name of the Simple Mail Transfer Protocol (SMTP) server.

Note: If you plan to set up an SMTP server for e-mail alert notifications, make sure that the name in the **Name** field in the ASM Information area of the System Settings window is valid as part of an e-mail address (for example, there are no spaces).

1. Log in to the Remote Supervisor Adapter II where you want to configure SMTP. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Network Protocols** and scroll down to the **SMTP** area.
3. In the **SMTP Server Host Name** or **IP Address** field, type the host name of the SMTP server. Use this field to specify the IP address or, if DNS is enabled and configured, the host name of the SMTP server.
4. Scroll to the bottom of the page and click **Save**.

Configuring LDAP

Using a Lightweight Directory Access Protocol (LDAP) server, a Remote Supervisor Adapter II can authenticate a user by querying or searching an LDAP directory on an LDAP server, instead of going through its local user database. Then, all Remote Supervisor Adapter IIs can remotely authenticate any user access through a central LDAP server. This requires LDAP client support on the Remote Supervisor Adapter II. You can also assign authority levels according to information that is found on the LDAP server.

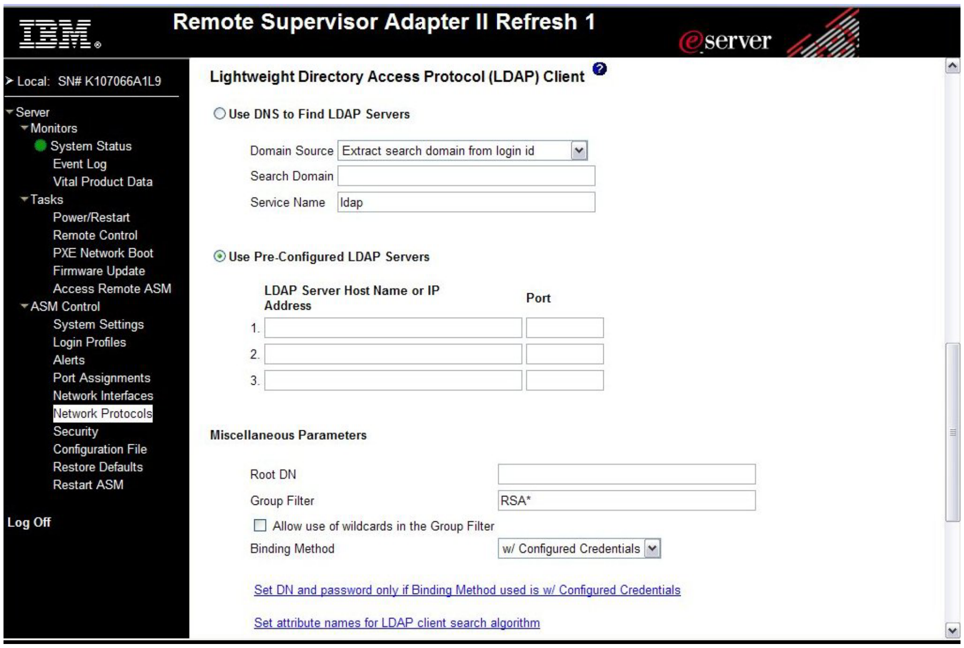
You can also use LDAP to assign users and Remote Supervisor Adapter IIs to groups and perform group authentication, in addition to the normal user (password check) authentication. For example, a Remote Supervisor Adapter II can be associated with one or more groups, and a user would pass group authentication only if the user belongs to at least one group that is associated with the Remote Supervisor Adapter II.

Note: LDAP-based authentication for PPP sessions is not supported.

Setting up a client to use the LDAP server

To set up a client to use the LDAP server, complete the following steps:

1. Log in to the Remote Supervisor Adapter II on which you want to set up the client. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Network protocols**. Scroll down to the **Lightweight Directory Access Protocol (LDAP) Client** area. A page similar to the one in the following illustration is displayed.



Lightweight Directory Access Protocol (LDAP) Client

○ Use DNS to Find LDAP Servers

Domain Source: Extract search domain from login id

Search Domain:

Service Name: ldap

● Use Pre-Configured LDAP Servers

	LDAP Server Host Name or IP Address	Port
1.		
2.		
3.		

Miscellaneous Parameters

Root DN:

Group Filter: RSA*

□ Allow use of wildcards in the Group Filter

Binding Method: w/ Configured Credentials

Set DN and password only if Binding Method used is w/ Configured Credentials

Set attribute names for LDAP client search algorithm

The Remote Supervisor Adapter II contains a Version 2.0 LDAP client that you can configure to provide user authentication through one or more LDAP servers. The LDAP server that is to be used for authentication can be discovered dynamically or manually preconfigured.

3. Choose one of the following methods to configure the LDAP client:
   - To dynamically discover the LDAP server, select **Use DNS to Find LDAP Servers**.

     If you choose to discover the LDAP server dynamically, the mechanisms that are described by RFC2782 (a DNS RR for specifying the location of services) are applied to find the server. This is known as DNS SRV. The parameters are described in the following list:

     Domain Source
     The DNS SRV request that is sent to the DNS server must specify a domain name. The LDAP client determines where to get this domain name according to which option is selected. There are three options:

     – **Extract search domain from login id**. The LDAP client uses the domain name in the login ID. For example, if the login ID is joesmith@mycompany.com, the domain name is mycompany.com. If the domain name cannot be extracted, the DNS SRV fails, causing the user authentication to fail automatically.

     – **Use only configured search domain below**. The LDAP client uses the domain name that is configured in the **Search Domain** parameter.

     – **Try login id first, then configured value**. The LDAP client first attempts to extract the domain name from the login ID. If this is successful, this domain name is used in the DNS SRV request. If no domain name is present in the login ID, the LDAP client uses the configured **Search Domain** parameter as the domain name in the DNS SRV request. If nothing is configured, user authentication fails immediately.

     Search Domain
     This parameter can be used as the domain name in the DNS SRV request, depending on how the **Domain Source** parameter is configured.

Service Name
The DNS SRV request that is sent to the DNS server must also specify a service name. The configured value is used. If this field is left blank, the default value is ldap. The DNS SRV request must also specify a protocol name. The default is tcp and is not configurable.

- To use a preconfigured LDAP server, select **Use Pre-Configured LDAP Server**.

Note: The port number for each server is optional. If the field is left blank, the default value of 389 is used for nonsecured LDAP connections. For secured connections, the default is 636. You must configure at least one LDAP server.

You can configure the following parameters:

Root DN
This is the distinguished name (DN) for the root entry of the directory tree on the LDAP server (for example, dn=mycompany,dc=com). This DN is used as the base object for all searches.

Group Filter
This field is used for group authentication. Group authentication is attempted after the user's credentials are successfully verified. If group authentication fails, the user's attempt to log on is denied. When the group filter is configured, it is used to specify to which groups this Service Processor belongs. This means that the user must belong to at least one of the groups that are configured for group authentication to succeed. If the **Group Filter** field is left blank, group authentication automatically succeeds. If the group filter is configured, an attempt is made to match at least one group in the list to a group to which the user belongs. If there is no match, the user fails authentication and is denied access. If there is at least one match, group authentication is successful. The comparisons are case sensitive.

The filter is limited to 511 characters and can consist of one or more group names. The colon (:) character must be used to delimit multiple group names. Leading and trailing spaces are ignored, but any other space is treated as part of the group name. A selection to allow or not allow the use of wildcards in the group name is provided. The filter can be a specific group name (for example, RSAWest), a wildcard (*) that matches everything, or a wildcard with a prefix (for example, RSA*). The default filter is RSA*. If security policies in your installation prohibit the use of wildcards, you can choose to not allow the use of wildcards, and the wildcard character (*) is treated as a normal character instead of the wildcard.

A group name can be specified as a full DN or using only the cn portion. For example, a group with a DN of cn=adminGroup,dc=mycompany,dc=com can be specified using the actual DN or with adminGroup.

For Active Directory environments only, nested group membership is supported. For example, if a user is a member of GroupA and GroupB, and GroupA is a member of GroupC, the user is said to be a member of GroupC also. Nested searches stop if 128 groups have been searched. Groups in one level are searched before groups in a lower level. Loops are not detected.

Binding Method
Before the LDAP server can be searched or queried, a bind request must be sent. This parameter controls how this initial bind to the LDAP server is performed. Choose from the following three options:

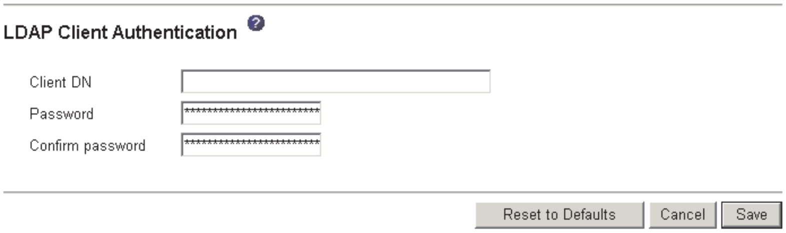
- **Anonymously**. Bind without a DN or password. This option is strongly discouraged because most servers are configured to not allow search requests on specific user records.
- **w/ Configured Credentials**. Bind with configured client DN and password.
- **w/ Login Credentials**. Bind with the credentials that are supplied during the login process. The user ID can be provided using a Distinguished Name, a fully qualified domain name, or through a user ID that matches the UID Search Attribute that is configured on the adapter.

If the initial bind is successful, a search is performed to find an entry on the LDAP server that belongs to the user who is logging in. If necessary, a second attempt to bind is attempted, this time with the DN that is retrieved from the user's LDAP record and the password that was entered during the login process. If this fails, the user is denied access. The second bind is performed only when the Anonymous or Configured Credentials binding methods are used.

Configuring the LDAP client authentication

To configure the LDAP client authentication, complete the following steps:

1. In the navigation pane, click **Network protocols**.
2. Scroll down to the **Lightweight Directory Access Protocol (LDAP) Client** area and click **Set DN and password only if Binding Method used is w/ Configured Credentials** area. A page similar to the one in the following illustration is displayed.



LDAP Client Authentication

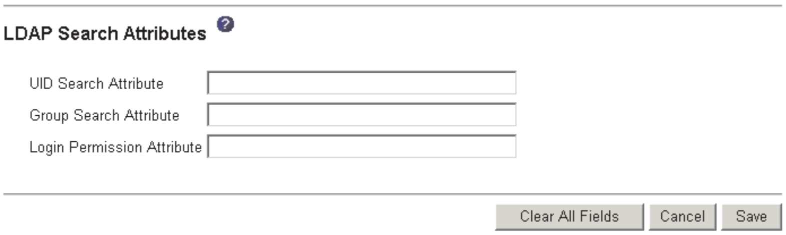
Client DN	
Password	*************************
Confirm password	*************************

3. To use client-based authentication, in the **Client DN** field, type a client distinguished name. Type a password in the **Password** field or leave it blank.

Configuring the LDAP search attributes

To configure the LDAP search attributes, complete the following steps:

1. In the navigation pane, click **Network protocols**.
2. Scroll down to the **Lightweight Directory Access Protocol (LDAP) Client** area and click **Set attribute names for LDAP client search algorithm**. A page similar to the one in the following illustration is displayed.


LDAP Search Attributes

UID Search Attribute

Group Search Attribute

Login Permission Attribute

3. To configure the search attributes, use the following information.

UID Search Attribute

When the selected binding method is **Anonymously** or **w/ Configured Credentials**, the initial bind to the LDAP server is followed by a search request that is directed at retrieving specific information about the user, including the distinguished name, login permissions, and group membership. To retrieve this information, the search request must specify the attribute name that is used to represent user IDs on that server. Specifically, this name is used as a search filter against the login ID that is entered by the user. This attribute name is configured here. For example, on Active Directory servers, the attribute name that is used for user IDs is usually sAMAccoutName. On Novell eDirectory and OpenLDAP servers, it is usually uid. If this field is left blank, a default of UID is used during user authentication.

Group Search Attribute

In an Active Directory or Novell eDirectory environment, this parameter specifies the attribute name that is used to identify the groups to which a user belongs. In Active Directory, this is usually memberOf, and with eDirectory, this is usually groupMembership.

In an OpenLDAP server environment, users are usually assigned to groups whose objectClass equals PosixGroup. In that context, this parameter specifies the attribute name that is used to identify the members of a particular PosixGroup. This is usually memberUid.

If this field is left blank, the attribute name in the filter defaults to memberOf.

Login Permission Attribute

When a user is authenticated through an LDAP server successfully, the login permissions for this user must be retrieved. To retrieve these permissions, the search filter that is sent to the server must specify the attribute name that is associated with login permissions. This field specifies this attribute name.

If this field is left blank, the user is assigned a default of read-only permissions, assuming that the user passes the user and group authentication.

The attribute value that is returned by the LDAP server is searched for the keyword string IBMRBSPermission=. This keyword must be immediately followed by a bit string that is entered as 12 consecutive 0s or 1s. Each bit represents a particular set of functions. The bits are numbered according to their positions. The leftmost bit is bit position 0, and the rightmost bit is bit position 11. A value of 1 at a particular position enables the function that is associated with that position. A value of 0 disables that function. The string IBMRBSPermission=010000000000 is a valid example.

The IBMRBSPermission= keyword is used to allow it to be placed anywhere in the attribute field. This enables the LDAP administrator to reuse an existing attribute, therefore preventing an extension to the LDAP schema. This also enables the attribute to be used for its original purpose. You can add the keyword string anywhere in the attribute field. The attribute that you use should allow for a free-formatted string.

When the attribute is retrieved successfully, the value that is returned by the LDAP server is interpreted according to the following information:

- **Deny Always (bit position 0):** If this bit is set, the user always fails authentication. This function can be used to block a particular user or users who are associated with a particular group.
- **Supervisor Access (bit position 1):** If this bit is set, the user is given administrator privileges. The user has read and write access to every function. When this bit is set, bits 2 through 11 do not have to be set individually.
- **Read Only Access (bit position 2):** If this bit is set, the user has read-only access and cannot perform any maintenance procedures (for example, restart, remote actions, and firmware updates) or modify anything (using the save, clear, or restore functions). The Read Only Access bit and all other bits are mutually exclusive, with the Read Only Access bit having the lowest precedence. If any other bit is set, the Read Only Access bit is ignored.
- **Networking and Security (bit position 3):** If this bit is set, the user can modify the configuration on the Security, Network Protocols, Network Interface, Port Assignments, and Serial Port pages.
- **User Account Management (bit position 4):** If this bit is set, the user can add, modify, and delete users and change the Global Login Settings in the Login Profiles page.
- **Remote Console Access (bit position 5):** If this bit is set, the user can access the remote server console.
- **Remote Console and Remote Disk (bit position 6):** If this bit is set, the user can access the remote server console and the remote disk functions for the remote server.
- **Remote Server Power/Restart Access (bit position 7):** If this bit is set, the user can access the power-on and restart functions for the remote server. These functions are available in the Power/Restart page.
- **Basic Adapter Configuration (bit position 8):** If this bit is set, the user can modify configuration parameters on the System Settings and Alerts pages.
- **Ability to Clear Event Logs (bit position 9):** If this bit is set, the user can clear the event logs. All users can view the event logs, but this particular permission is required to clear the logs.
- **Advanced Adapter Configuration (bit position 10):** If this bit is set, the user has no restrictions when configuring the adapter. In addition, the user is said to have administrative access to the Remote Supervisor Adapter II, meaning that the user can also perform the following advanced functions: firmware upgrades, PXE network boot, restoring adapter factory defaults, modifying and restoring adapter configuration from a configuration file, and restarting and resetting the adapter.
- **Reserved (bit position 11):** This bit is reserved for future use.

If none of the bits are set, the user has read-only authority.

Priority is given to login permissions that are retrieved directly from the user record. If the login permission attribute is not in the user's record, an attempt is made to retrieve the permissions from the groups to which the user belongs. This is done as part of the group authentication phase. The user is assigned the inclusive OR of all the bits for all of the groups. The Read Only bit is set only if all the other bits are zero. If the Deny Always bit is set for any of the groups, the user is refused access. The Deny Always bit always has precedence over every other bit.

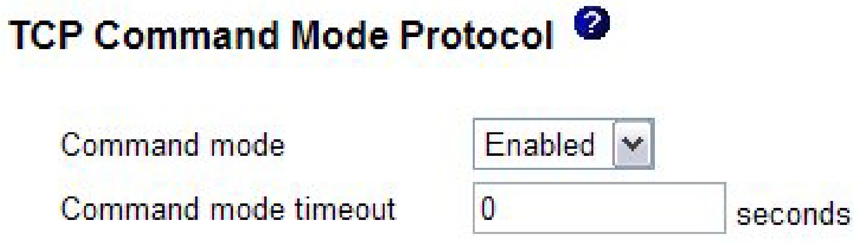
Important: If you give a user the ability to modify basic, networking, and security-related adapter configuration parameters, consider giving this same user the ability to restart the Remote Supervisor Adapter II (bit position 10). Otherwise, a user might be able to change parameters (for example, the IP address of the adapter) but will not be able to make them take effect.

TCP Command Mode Protocol

The TCP Command Mode Protocol is used by IBM Director for out-of-band communication with the Remote Supervisor Adapter II.

To set up TCP command mode, complete the following steps:

1. In the navigation pane, click **Network protocols**.
2. Scroll down to the **TCP Command Mode Protocol** area. A page similar to the one in the following illustration is displayed.



TCP Command Mode Protocol

Command mode: Enabled

Command mode timeout: 0 seconds

3. You can configure the following parameters:

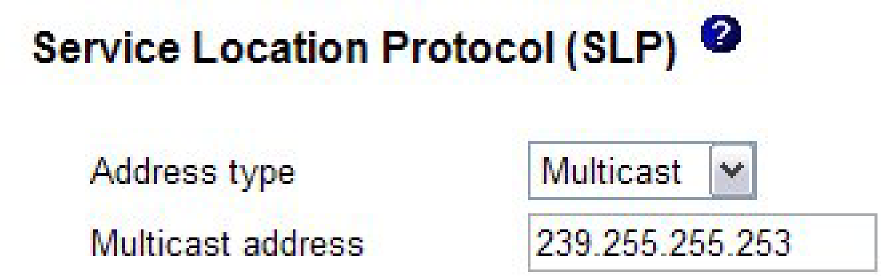
Command mode
You can use this field to specify whether you want to allow TCP command mode sessions to connect to the Remote Supervisor Adapter II. The default is **Enabled**.

Command mode timeout
This is the TCP command mode inactivity timeout, in seconds. If there is no traffic from a TCP command mode session for the specified number of seconds, the Remote Supervisor Adapter II closes the connection. A value of 0 (the default) means that there is no timeout.

Service Location Protocol (SLP)

To set up the Service Location Protocol (SLP), complete the following steps:

1. In the navigation pane, click **Network protocols**.
2. Scroll down to the **Service Location Protocol (SLP)** area. A page similar to the one in the following illustration is displayed.



Service Location Protocol (SLP)

Address type: Multicast

Multicast address: 239.255.255.253

3. You can configure the following parameters:

   Address type
   This is the address type that the MM SLP server listens on. If **Broadcast** is selected, the SLP server listens on the broadcast address of 255.255.255.255. If **Multicast** is selected, the SLP server listens on the IP address that is specified in the **Multicast address** field. The default for this field is **Multicast**.

   Multicast address
   This is the multicast IP address that the MM SLP server listens on if the **Address type** field is set to **Multicast**. The default multicast address is 239.255.255.253. If you change this address, you must enter a multicast IP address (its first byte must be between 224 and 239).

Secure Web server and secure LDAP

Secure Sockets Layer (SSL) is a security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

You can configure the Remote Supervisor Adapter II to use SSL support for two types of connections: secure Web server (HTTPS) and secure LDAP connection (LDAPS). The Remote Supervisor Adapter II takes on the role of SSL client or SSL server depending on the type of connection. The following table shows that the Remote Supervisor Adapter II acts as an SSL server for secure Web server connections. The Remote Supervisor Adapter II acts as an SSL client for secure LDAP connections.

Table 10. Remote Supervisor Adapter II SSL connection support

Connection type	SSL client	SSL server
Secure Web server (HTTPS)	Web browser of the user (For example: Microsoft Internet Explorer)	A Remote Supervisor Adapter II Web server
Secure LDAP connection (LDAPS)	Remote Supervisor Adapter II LDAP client	An LDAP server

You can view or change the Secure Sockets Layer (SSL) settings from the Security page. You can enable or disable SSL and manage the certificates that are required for SSL.

Configuring security

Use the general procedure in this section to configure security for the Remote Supervisor Adapter II Web server and to configure security for the connection between the Remote Supervisor Adapter II and an LDAP server. If you are not familiar with the use of SSL certificates, read the information in “SSL certificate overview.”

Use the following general tasks list to configure the security for the Remote Supervisor Adapter II:

1. Configure the Secure Web server:
   a. Disable the SSL server. Use the **SSL Server Configuration for Web Server** area on the Security page.
   b. Generate or import a certificate. Use the **SSL Server Certificate Management** area on the Security page. (See “SSL server certificate management” on page 55.)
   c. Enable the SSL server. Use the **SSL Server Configuration for Web Server** area on the Security page. (See “Enabling SSL for the secure Web server” on page 60.)
2. Configure SSL security for LDAP connections:
   a. Disable the SSL client. Use the **SSL Client Configuration for LDAP Client** area on the Security page.
   b. Generate or import a certificate. Use the **SSL Client Certificate Management** area on the Security page. (See “SSL client certificate management” on page 60.)
   c. Import one or more trusted certificates. Use the **SSL Client Trusted Certificate Management** area on the Security page. (See “SSL client trusted certificate management” on page 61.)
   d. Enable the **SSL client. Use the SSL Client Configuration for LDAP Client** area on the Security page. (See “Enabling SSL for the LDAP client” on page 62.)
3. Restart the Remote Supervisor Adapter II for SSL server configuration changes to take effect. For more information, see “Restarting ASM” on page 66.

   Note: Changes to the SSL client configuration take effect immediately and do not require a restart of the Remote Supervisor Adapter II.

SSL certificate overview

You can use SSL with either a self-signed certificate or with a certificate that is signed by a third-party certificate authority. Using a self-signed certificate is the simplest method for using SSL, but it does create a small security risk. The risk arises because the SSL client has no way of validating the identity of the SSL server for the first connection that is attempted between the client and server. It is possible that a third party could impersonate the server and intercept data that is flowing between the Remote Supervisor Adapter II and the Web browser. If, at the time of the initial connection between the browser and the Remote Supervisor Adapter II, the self-signed certificate is imported into the certificate store of the browser, all future communications will be secure for that browser (assuming that the initial connection was not compromised by an attack).

For more complete security, you can use a certificate that is signed by a certificate authority. To obtain a signed certificate, use the SSL Certificate Management page to generate a certificate-signing request. You must then send the certificate-signing request to a certificate authority and make arrangements to procure a certificate. When the certificate is received, it is then imported into the Remote Supervisor Adapter II through the **Import a Signed Certificate** link, and you can enable SSL.

The function of the certificate authority is to verify the identity of the Remote Supervisor Adapter II. A certificate contains digital signatures for the certificate authority and the Remote Supervisor Adapter II. If a well-known certificate authority issues the certificate or if the certificate of the certificate authority has already been imported into the Web browser, the browser will be able to validate the certificate and positively identify the Remote Supervisor Adapter II Web server.

The Remote Supervisor Adapter II requires a certificate for the secure Web server and one for the secure LDAP client. Also, the secure LDAP client requires one or more trusted certificates. The trusted certificate is used by the secure LDAP client to positively identify the LDAP server. The trusted certificate is the certificate of the certificate authority that signed the certificate of the LDAP server. If the LDAP server uses self-signed certificates, the trusted certificate can be the certificate of the LDAP server itself. Additional trusted certificates must be imported if more than one LDAP server is used in your configuration.

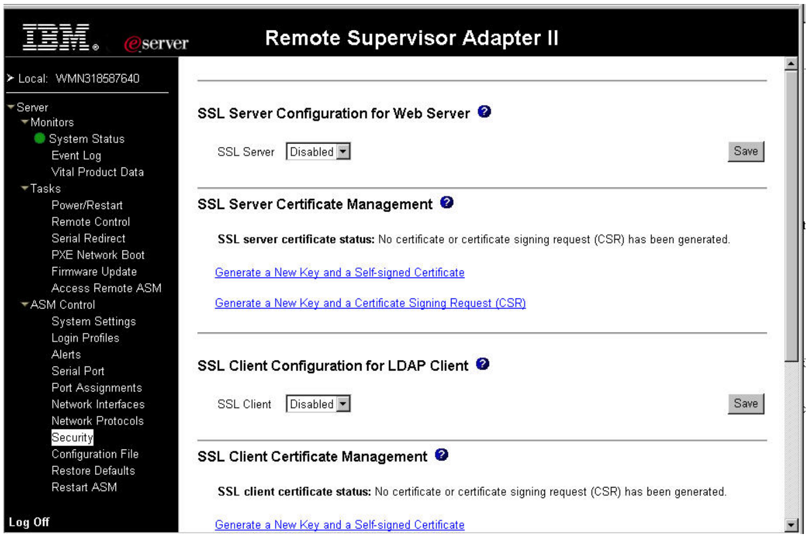
SSL server certificate management

The SSL server requires that a valid certificate and corresponding private encryption key be installed before SSL is enabled. Two methods are available for generating the private key and required certificate: using a self-signed certificate and using a certificate that is signed by a certificate authority. If you want to use a self-signed certificate for the SSL server, see “Generating a self-signed certificate.” If you want to use a certificate-authority-signed certificate for the SSL server, see “Generating a certificate-signing request” on page 56.

Generating a self-signed certificate

To generate a new private encryption key and self-signed certificate, complete the following steps:

1. In the navigation plane, click **Security**. A page similar to the one in the following illustration is displayed.



SSL Server Configuration for Web Server

SSL Server Disabled Save

SSL Server Certificate Management

SSL server certificate status: No certificate or certificate signing request (CSR) has been generated.

Generate a New Key and a Self-signed Certificate

Generate a New Key and a Certificate Signing Request (CSR)

SSL Client Configuration for LDAP Client

SSL Client Disabled Save

SSL Client Certificate Management

SSL client certificate status: No certificate or certificate signing request (CSR) has been generated.

Generate a New Key and a Self-signed Certificate

2. In the SSL Server Configuration for Web Server area, make sure that the SSL server is disabled. If it is not disabled, select **Disabled** in the **SSL Server** field and then click **Save**.

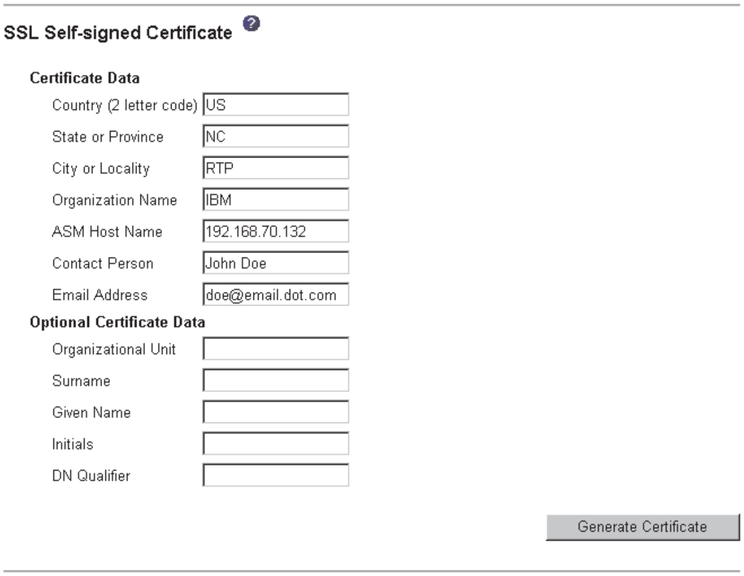
   Notes:

   a. The Remote Supervisor Adapter II must be restarted before the selected value (Enabled or Disabled) takes effect.

b. Before you can enable SSL, a valid SSL certificate must be in place.

c. To use SSL, you must configure a client Web browser to use SSL3 or TLS. Older export-grade browsers with only SSL2 support cannot be used.

3. In the SSL Server Certificate Management area, select **Generate a New Key and a Self-signed Certificate**. A page similar to the one in the following illustration is displayed.



SSL Self-signed Certificate

Certificate Data

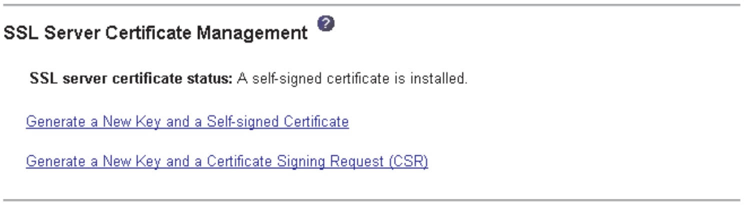
Country (2 letter code)	US
State or Province	NC
City or Locality	RTP
Organization Name	IBM
ASM Host Name	192.168.70.132
Contact Person	John Doe
Email Address	doe@email.dot.com

Optional Certificate Data

Organizational Unit	
Surname	
Given Name	
Initials	
DN Qualifier	

4. Type the information in the required fields and any optional fields that apply to your configuration. For a description of the fields, see “Required certificate data” on page 57. After you finish typing the information, click **Generate Certificate**. Your new encryption keys and certificate are generated. This process might take several minutes.

   A page similar to the one in the following illustration is displayed and you can see that a self-signed certificate is installed.



SSL Server Certificate Management

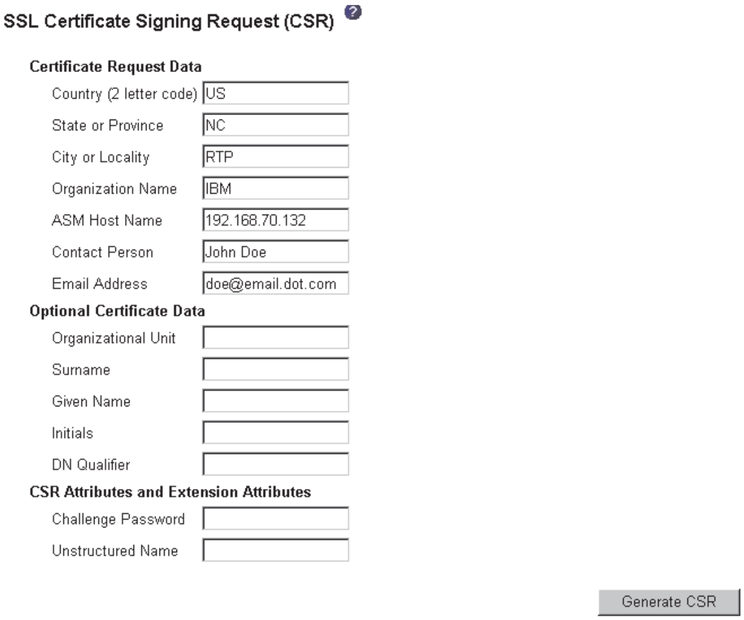
SSL server certificate status: A self-signed certificate is installed.

Generate a New Key and a Self-signed Certificate
Generate a New Key and a Certificate Signing Request (CSR)

Generating a certificate-signing request

To generate a new private encryption key and certificate-signing request, complete the following steps:

1. In the navigation pane, click **Security**.
2. In the SSL Server Configuration for Web Server area, make sure that the SSL server is disabled. If it is not disabled, select **Disabled** in the **SSL Server** field and then click **Save**.
3. In the SSL Server Certificate Management area, select **Generate a New Key and a Certificate-Signing Request**. A page similar to the one in the following illustration is displayed.



SSL Certificate Signing Request (CSR)

Certificate Request Data

Country (2 letter code)	US
State or Province	NC
City or Locality	RTP
Organization Name	IBM
ASM Host Name	192.168.70.132
Contact Person	John Doe
Email Address	doe@email.dot.com

Optional Certificate Data

Organizational Unit	
Surname	
Given Name	
Initials	
DN Qualifier	

CSR Attributes and Extension Attributes

Challenge Password	
Unstructured Name	

4. Type the information in the required fields and any optional fields that apply to your configuration. The fields are the same as for the self-signed certificate, with some additional fields.

   Read the information in the following sections for a description of each of the common fields.

   Required certificate data
   The following user-input fields are required for generating a self-signed certificate or a certificate-signing request:

   Country
   Use this field to indicate the country where the Remote Supervisor Adapter II is physically located. This field must contain the 2-character country code.

   State or Province
   Use this field to indicate the state or province where the Remote Supervisor Adapter II is physically located. This field can contain a maximum of 30 characters.

   City or Locality
   Use this field to indicate the city or locality where the Remote Supervisor Adapter II is physically located. This field can contain a maximum of 50 characters.

   Organization Name
   Use this field to indicate the company or organization that owns the Remote Supervisor Adapter II. When this is used to generate a certificate-signing request, the issuing certificate authority can verify that the organization that is requesting the certificate is legally entitled to claim ownership of the given company or organization name. This field can contain a maximum of 60 characters.

   ASM Host Name
   Use this field to indicate the Remote Supervisor Adapter II host name that currently appears in the browser Web address bar.

   Make sure that the value that you typed in the **ASM host name** field exactly matches the host name as it is known by the Web browser. The browser compares the host name in the resolved

Web address to the name that appears in the certificate. To prevent certificate warnings from the browser, the value that is used in this field must match the host name that is used by the browser to connect to the Remote Supervisor Adapter II. For example, if the address in the Web address bar is http://mm11.xyz.com/private/main.ssi, the value that is used for the **ASM Host Name** field must be mm11.xyz.com. If the Web address is http://mm11/private/main.ssi, the value that is used must be mm11. If the Web address is http://192.168.70.2/private/main.ssi, the value that is used must be 192.168.70.2.

This certificate attribute is generally referred to as the common name.

This field can contain a maximum of 60 characters.

Contact Person
Use this field to indicate the name of a contact person who is responsible for the Remote Supervisor Adapter II. This field can contain a maximum of 60 characters.

Email Address
Use this field to indicate the e-mail address of a contact person who is responsible for the Remote Supervisor Adapter II. This field can contain a maximum of 60 characters.

Optional certificate data
The following user-input fields are optional for generating a self-signed certificate or a certificate-signing request:

Organizational Unit
Use this field to indicate the unit within the company or organization that owns the Remote Supervisor Adapter II. This field can contain a maximum of 60 characters.

Surname
Use this field for additional information, such as the surname of a person who is responsible for the Remote Supervisor Adapter II. This field can contain a maximum of 60 characters

Given Name
Use this field for additional information, such as the given name of a person who is responsible for the Remote Supervisor Adapter II. This field can contain a maximum of 60 characters.

Initials
Use this field for additional information, such as the initials of a person who is responsible for the Remote Supervisor Adapter II. This field can contain a maximum of 20 characters.

DN Qualifier
Use this field for additional information, such as a distinguished name qualifier for the Remote Supervisor Adapter II. This field can contain a maximum of 60 characters.

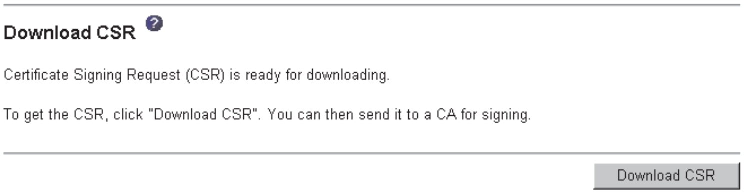
Certificate-Signing request attributes
The following fields are optional unless they are required by your selected certificate authority:

Challenge Password
Use this field to assign a password to the certificate-signing request. This field can contain a maximum of 30 characters.

Unstructured Name
Use this field for additional information, such as an unstructured

name that is assigned to the Remote Supervisor Adapter II. This field can contain a maximum of 60 characters.

5. After completing the information, click **Generate CSR**. The new encryption keys and certificate are generated. This process might take several minutes. A page similar to the one in the following illustration is displayed when the process is completed.



Download CSR

Certificate Signing Request (CSR) is ready for downloading.

To get the CSR, click "Download CSR". You can then send it to a CA for signing.

6. Click **Download CSR** and then click **Save** to save the file to your workstation. The file that is produced when you create a certificate-signing request is in DER format. If your certificate authority expects the data in some other format, such as PEM, the file can be converted using a tool such as OpenSSL (http://www.openssl.org). If the certificate authority asks you to copy the contents of the certificate-signing request file into a Web browser window, PEM format is usually expected.

   The command for converting a certificate-signing request from DER to PEM format using OpenSSL is similar to the following example:

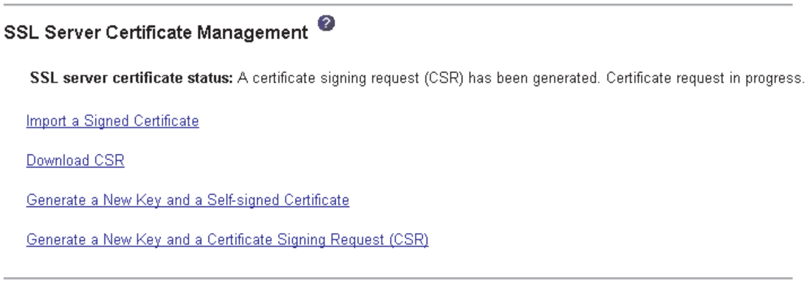
   ```
   openssl req -in csr.der -inform DER -out csr.pem -outform PEM
   ```

7. Send the certificate-signing request to your certificate authority. When the certificate authority returns your signed certificate, you might have to convert the certificate to DER format. (If you received the certificate as text in an e-mail or a Web page, it is probably in PEM format.) You can change the format using a tool that is provided by your certificate authority or using a tool such as OpenSSL (http://www.openssl.org). The command for converting a certificate from PEM to DER format is similar to the following example:

   ```
   openssl x509 -in cert.pem -inform PEM -out cert.der -outform DER
   ```

   Go to step 8 after the signed certificate is returned from the certificate authority.

8. In the navigation pane, click **Security**. Scroll to the **SSL Server Certificate Management** area, which looks similar to the page in the following illustration.

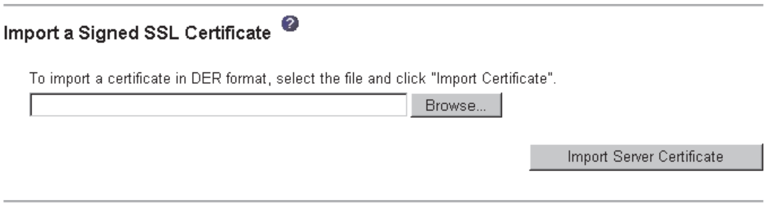


SSL Server Certificate Management

SSL server certificate status: A certificate signing request (CSR) has been generated. Certificate request in progress.

Import a Signed Certificate
Download CSR
Generate a New Key and a Self-signed Certificate
Generate a New Key and a Certificate Signing Request (CSR)

9. Click **Import a Signed Certificate**. A page similar to the one in the following illustration is displayed.


Import a Signed SSL Certificate

To import a certificate in DER format, select the file and click "Import Certificate".

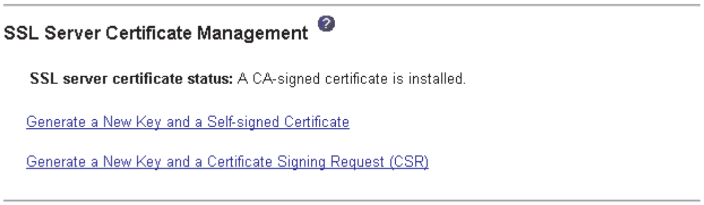
10. Click **Browse**.
11. Click the certificate file that you want and then click **Open**. The file name (including the full path) is displayed in the field next to the **Browse** button.
12. Click **Import Server Certificate** to begin the process. A progress indicator is displayed as the file is transferred to storage on the Remote Supervisor Adapter II. Continue to display this page until the transfer is completed.

Enabling SSL for the secure Web server

Note: To enable SSL, you must have a valid SSL certificate installed.

Complete the following steps to enable the secure Web server:

1. In the navigation pane, click **Security**. The page that is displayed looks similar to the one in the following illustration and shows that a valid SSL server certificate is installed. If the SSL server certificate status does not show that a valid SSL certificate is installed, go to “SSL server certificate management” on page 55.


SSL Server Certificate Management

SSL server certificate status: A CA-signed certificate is installed.

Generate a New Key and a Self-signed Certificate
Generate a New Key and a Certificate Signing Request (CSR)

2. Scroll to the **SSL Server Configuration for Web Server** area, select **Enabled** in the **SSL Client** field, and then click **Save**. The selected value takes effect the next time the Remote Supervisor Adapter II is restarted.

SSL client certificate management

The SSL client requires that a valid certificate and corresponding private encryption key be installed before SSL is enabled. Two methods are available for generating the private key and required certificate: using a self-signed certificate, or using a certificate signed by a certificate authority.

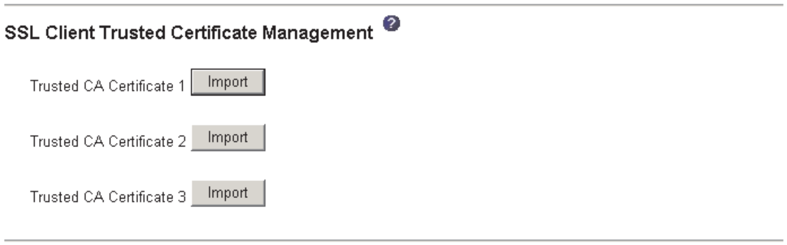
The procedure for generating the private encryption key and certificate for the SSL client is the same as the procedure for the SSL server, except that you use the **SSL Client Certificate Management** area of the Security Web page instead of the **SSL Server Certificate Management** area. If you want to use a self-signed certificate for the SSL client, see “Generating a self-signed certificate” on page 55. If you want to use a certificate authority signed certificate for the SSL client, see “Generating a certificate-signing request” on page 56.

SSL client trusted certificate management

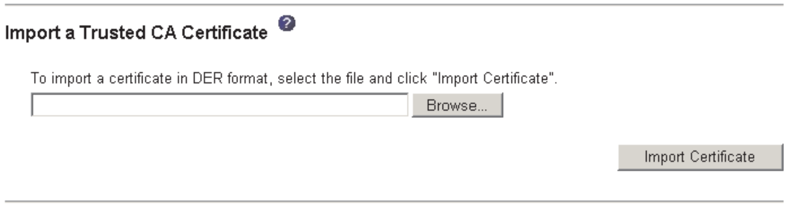
The secure SSL client (LDAP client) uses trusted certificates to positively identify the LDAP server. A trusted certificate can be the certificate of the certificate authority that signed the certificate of the LDAP server, or it can be the actual certificate of the LDAP server. At least one certificate must be imported to the Remote Supervisor Adapter II before the SSL client is enabled. You can import up to three trusted certificates.

To import a trusted certificate, complete the following steps:

1. In the navigation pane, select **Security**.
2. In the SSL Client Configuration for LDAP Client area, make sure that the SSL client is disabled. If it is not disabled, select **Disabled** in the **SSL Client** field and then click **Save**.
3. Scroll to the SSL Client Trusted Certificate Management area. A page similar to the one in the following illustration is displayed.



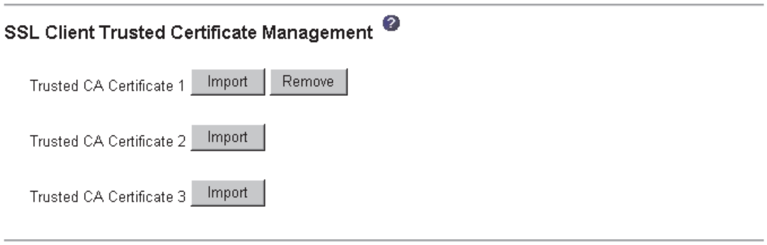
4. Click **Import** next to one of the **Trusted CA Certificate 1** fields. A page similar to the one in the following illustration is displayed.



To import a certificate in DER format, select the file and click "Import Certificate".

5. Click **Browse**.
6. Select the certificate file that you want and click **Open**. The file name (including the full path) is displayed in the box beside the **Browse** button.
7. To begin the import process, click **Import Certificate**. A progress indicator is displayed as the file is transferred to storage on the Remote Supervisor Adapter II. Continue displaying this page until the transfer is completed.

   The SSL Client Trusted Certificate Management area of the Security page now look similar to the one in the following illustration.



The **Remove** button is now available for the Trusted CA Certificate 1 option. If you want to remove a trusted certificate, click the corresponding **Remove** button.

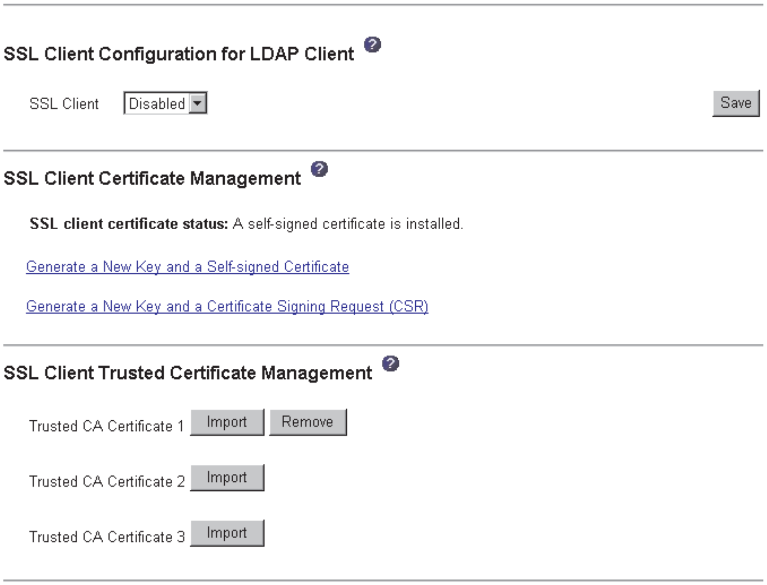
You can import other trusted certificates using the Trusted CA Certificate 2 and the Trusted CA Certificate 3 **Import** buttons.

Enabling SSL for the LDAP client

Use the SSL Client Configuration for LDAP Client area of the Security page to enable or disable SSL for the LDAP Client. To enable SSL, a valid SSL client certificate and at least one trusted certificate must first be installed.

To enable SSL for the client, complete the following steps:

1. In the navigation pane, click **Security**. A page similar to the one in the following illustration is displayed.



SSL Client Configuration for LDAP Client

SSL Client: Disabled

SSL Client Certificate Management

SSL client certificate status: A self-signed certificate is installed.

SSL Client Trusted Certificate Management

Save
Generate a New Key and a Self-signed Certificate
Generate a New Key and a Certificate Signing Request (CSR)
Trusted CA Certificate 1
Import
Remove
Trusted CA Certificate 2
Import
Trusted CA Certificate 3
Import

   The Security page shows an installed SSL client certificate and Trusted CA Certificate 1.

2. On the SSL Client Configuration for LDAP Client page, select **Enabled** in the **SSL Client** field.

   Notes:

   a. The selected value (Enabled or Disabled) takes effect immediately.

   b. Before you can enable SSL, a valid SSL certificate must be in place.

   c. Your LDAP server must support SSL3 or TLS to be compatible with the SSL implementation that the LDAP client uses.

3. Click **Save**. The selected value takes effect immediately.

Configuring the Secure Shell server

Note: The Secure Shell server feature is not available on all servers.

The Secure Shell (SSH) feature provides secure access to the command-line interface and the serial (text console) redirect features of the Remote Supervisor Adapter II.

Secure Shell users are authenticated by exchanging user ID and password. The password and user ID are sent after the encryption channel is established. The user ID and password pair can be one of the 12 locally stored user IDs and passwords, or they can be stored on an LDAP server. Public key authentication is not supported.

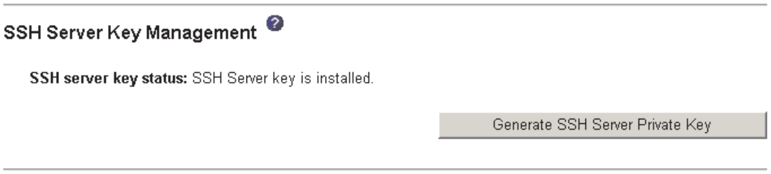
Generating a Secure Shell server key

A Secure Shell server key is used to authenticate the identity of the Secure Shell server to the client. Secure shell must be disabled before you create a new Secure Shell server private key. You must create a server key before enabling the Secure Shell server.

When you request a new server key, both a Rivest, Shamir, and Adelman key and a DSA key are created to allow access to the Remote Supervisor Adapter II from either an SSH version 1.5 or an SSH version 2 client. For security, the Secure Shell server private key is not backed up during a configuration save and restore operation.

To create a new Secure Shell server key, complete the following steps:

1. In the navigation pane, click **Security**.
2. Scroll to the **Secure Shell (SSH) Server** area and make sure that the Secure Shell server is disabled. If it is not disabled, select **Disabled** in the **SSH Server** field and then click **Save**.
3. Scroll to the **SSH Server Key Management** area. A page similar to the one in the following illustration is displayed.


SSH Server Key Management

SSH server key status: SSH Server key is installed.

4. Click **Generate SSH Server Private Key**. A progress window opens. Wait for the operation to be completed.

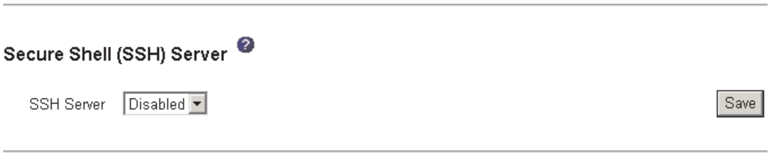
Enabling the Secure Shell server

From the Security page you can enable or disable the Secure Shell server. The selection that you make takes effect only after the Remote Supervisor Adapter II is restarted. The value that is displayed on the screen (Enabled or Disabled) is the last selected value and is the value that is used when the Remote Supervisor Adapter II is restarted.

Note: You can enable the Secure Shell server only if a valid Secure Shell server private key is installed.

To enable the Secure Shell server, complete the following steps:

1. In the navigation pane, click **Security**.
2. Scroll to the **Secure Shell (SSH) Server** area. A page similar to the one in the following illustration is displayed.



Secure Shell (SSH) Server

SSH Server: Disabled

3. Click **Enabled** in the **SSH Server** field.
4. In the navigation pane, click **Restart ASM** to restart the Remote Supervisor Adapter II.

Using the Secure Shell server

If you are using the Secure Shell client that is included in Red Hat Linux version 7.3, to start a Secure Shell session to a Remote Supervisor Adapter II with network address 192.168.70.132, type a command similar to the following example:

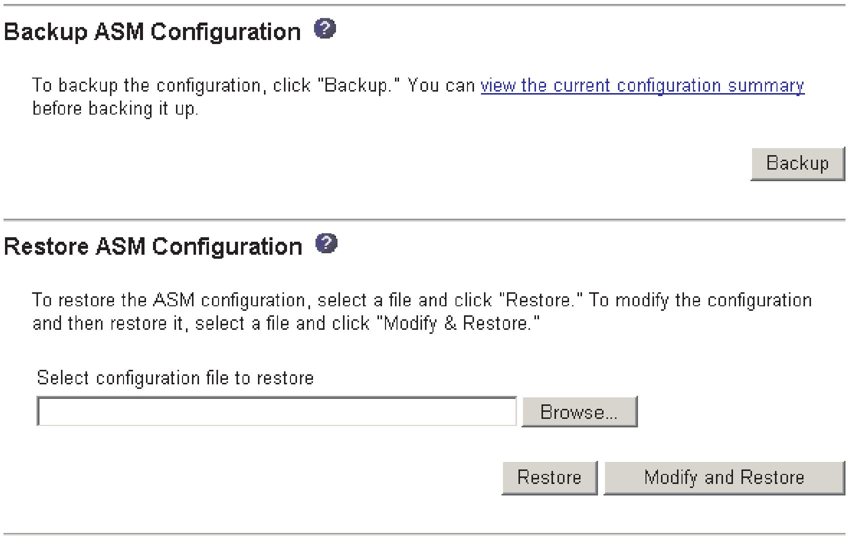
```
ssh -x -l userid 192.168.70.132
```

where -x indicates no X Window System forwarding and -l indicates that the session should use the user ID *userid*.

Using the configuration file

Select **Configuration File** in the navigation pane to back up and restore the ASM configuration:

Important: Security page settings are not saved with the backup operation and cannot be restored with the restore operation.



Backup ASM Configuration

To backup the configuration, click "Backup." You can view the current configuration summary before backing it up.

Restore ASM Configuration

To restore the ASM configuration, select a file and click "Restore." To modify the configuration and then restore it, select a file and click "Modify & Restore."

Select configuration file to restore

Backing up your current configuration

You can download a copy of your current ASM configuration to the client computer that is running the Remote Supervisor Adapter II Web interface. Use this backup copy to restore your Remote Supervisor Adapter II configuration if it is accidentally changed or damaged. Use it as a base that you can modify to configure multiple Remote Supervisor Adapter IIs with similar configurations.

To back up your current configuration, complete the following steps:

1. Log in to the Remote Supervisor Adapter II where you want to back up your current configuration. For more information, see Chapter 2, "Opening and using the Web interface," on page 5.
2. In the navigation pane, click **Configuration File**.
3. In the **Backup ASM Configuration** area, click **view the current configuration summary**.
4. Verify the settings and then click **Close**.
5. To back up this configuration, click **Backup**.
6. Type a name for the backup, select the location where the file will be saved, and then click **Save**.

   In Netscape Navigator, click **Save File**.

   In Microsoft Internet Explorer, click **Save this file to disk**, then click **OK**.

Restoring and modifying your ASM configuration

You can restore a saved configuration in full, or you can modify key fields in the saved configuration before restoring the configuration to your Remote Supervisor Adapter II. By modifying the configuration file before restoring it, you can set up multiple Remote Supervisor Adapter IIs with similar configurations. You can quickly specify parameters that require unique values such as names and IP addresses, without having to enter common, shared information.

To restore or modify your current configuration, complete the following steps:

1. Log in to the Remote Supervisor Adapter II where you want to restore the configuration. For more information, see Chapter 2, "Opening and using the Web interface," on page 5.
2. In the navigation pane, click **Configuration File**.
3. In the Restore ASM Configuration area, click **Browse**.
4. Click the configuration file that you want; then, click **Open**. The file (including the full path) appears in the box beside **Browse**.
5. If you do not want to make changes to the configuration file, click **Restore**. A new window opens with the ASM configuration information. Make sure that this is the configuration that you want to restore. If it is not the correct configuration, click **Cancel**.

   If you want to make changes to the configuration file before restoring, click **Modify and Restore** to open an editable configuration summary window. Initially, only the fields that allow changes appear. To change between this view and the complete configuration summary view, click the **Toggle View** button at the top or bottom of the window. To modify the contents of a field, click the corresponding text box and enter the data.

   Note: When you click **Restore** or **Modify and Restore**, an alert window might open if the configuration file that you are attempting to restore was created by a different type of service processor or was created by the same type of service processor with older firmware (and therefore, has less functionality). This alert message will include a list of system-management functions that you will have to configure after the restoration is complete. Some functions require configurations on more than one window.
6. To continue restoring this file to the Remote Supervisor Adapter II, click **Restore Configuration**. A progress indicator appears as the firmware on the Remote Supervisor Adapter II is updated. A confirmation window opens to verify whether the update was successful.

Note: The security settings on the Security page are not restored by the restore operation. To modify security settings, see “Secure Web server and secure LDAP” on page 53.

7. After receiving a confirmation that the restore process is complete, in the navigation pane, click **Restart ASM**; then, click **Restart**.
8. Click **OK** to confirm that you want to restart your Remote Supervisor Adapter II.
9. Click **OK** to close the current browser window.
10. To log in to the Remote Supervisor Adapter II again, start your browser, and follow your regular login process.

Restoring ASM defaults

Use the **Restore Defaults** link to restore the default configuration of the Remote Supervisor Adapter II, if you have read/write access.

Attention: When you click **Restore Defaults**, you will lose all the modifications that you made to the Remote Supervisor Adapter II. You also will lose the remote control of the remote servers.

To restore the ASM defaults, complete the following steps:

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Restore Defaults** to restore default settings of the Remote Supervisor Adapter II. If this is a local system, your TCP/IP connection will be broken, and you must reconfigure the network interface to restore connectivity.
3. Log in again to use the Remote Supervisor Adapter II Web interface.
4. Reconfigure the network interface to restore connectivity. For information about the network interface, see “Configuring an Ethernet connection to the Remote Supervisor Adapter II” on page 39.

Restarting ASM

Use the **Restart ASM** link to restart the Remote Supervisor Adapter II. You can perform this function only if you have read/write access. Any TCP/IP, modem, or interconnect connections are temporarily dropped. You must log in again to use the Remote Supervisor Adapter II Web interface.

To restart the Remote Supervisor Adapter II or ISMP, complete the following steps:

1. In the navigation pane, click **Restart ASM** to restart a Remote Supervisor Adapter II or ISMP. Your TCP/IP or modem connections are broken.
2. Log in again to use the Remote Supervisor Adapter II Web interface.

Logging off

Complete the following steps to log off the Remote Supervisor Adapter II or another remote server:

1. In the navigation pane, click **Log Off**.

   Note: If you are logged in to another remote server, you must first select **Log Off Remote ASM**.

2. If you are running Internet Explorer or Netscape Navigator, click **Yes** in the confirmation window.

   The current browser window closes to maintain security. You must manually close other open browser windows, if any, to prevent a cached version of your user ID and password from remaining available.

Chapter 4. Monitoring remote server status

Use the links under the **Monitors** heading of the navigation pane to view the status of the server that you are accessing.

From the System Status pages, you can:

- Monitor the power status of the server and view the state of the operating system
- View the server temperature readings, voltage thresholds, and fan speeds
- View the latest server operating-system-failure screen capture
- View the list of users who are logged in to the Remote Supervisor Adapter II

From the Event Log page, you can:

- View certain Advanced System Management events that are recorded in the event log of the Remote Supervisor Adapter II
- View the severity of events

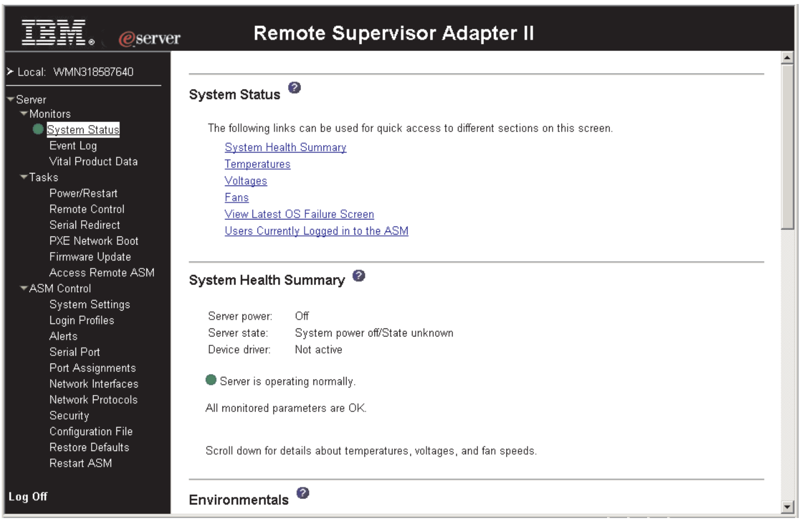
From the Vital Product Data (VPD) page, you can view the vital product data of the Remote Supervisor Adapter II, the server in which it is installed, and the ISMP.

Viewing system health

On the System Health Summary page, you can monitor the temperature readings, voltage thresholds, and fan status of your server.

To view the system health and environmental information of the server, complete the following steps:

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **System Status** to view a dynamically-generated update of the overall health of the server. A page similar to the one in the following illustration is displayed.



System Status

The following links can be used for quick access to different sections on this screen.

System Health Summary
Temperatures
Voltages
Fans
View Latest OS Failure Screen
Users Currently Logged in to the ASM

System Health Summary

Server power: Off
Server state: System power off/State unknown
Device driver: Not active

● Server is operating normally.

All monitored parameters are OK.

Scroll down for details about temperatures, voltages, and fan speeds.

Environmentals

The status of your server determines the message that is shown at the top of the System Health Summary page. One of the following symbols appears:

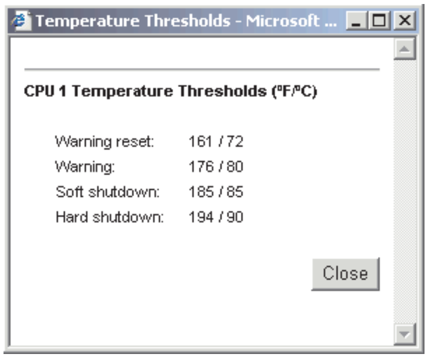
- A solid green circle and the phrase `Server is operating normally`

- Either a red circle that contains an X or a yellow triangle that contains an exclamation point and the phrase `One or more monitored parameters are abnormal`

  If the monitored parameters are operating outside normal ranges, a list of the specific abnormal parameters is displayed on the System Health Summary page.

3. Scroll down to the **Temperatures** area. The Remote Supervisor Adapter II tracks the current temperature readings and threshold levels for system components such as microprocessors, system board, and hard disk drive backplane.

   When you click a temperature reading, a window similar to the one in the following illustration opens.

   CPU 1 Temperature Thresholds (ºF/ºC)

   Warning reset: 161 / 72
   Warning: 176 / 80
   Soft shutdown: 185 / 85
   Hard shutdown: 194 / 90

   The Temperature Thresholds page displays the temperature levels at which the Remote Supervisor Adapter II reacts. The temperature threshold values are preset on the remote server and cannot be changed.

   The reported temperatures for the microprocessor (CPU), hard disk drive, and server are measured against the following threshold ranges:

   Warning Reset
   If a warning was sent and the temperature returns to any value below the warning reset value, the server assumes that the temperature has returned to normal, and no further alerts are generated.

   Warning
   When the temperature reaches a specified value, a temperature alert is sent to configured remote alert recipients. You must select the **Temperature** check box on the Alerts page for the alert to be sent.

   For more information about selecting Alert options, see "Setting remote alerts" on page 27.

   Soft Shutdown
   When the temperature reaches a specified value higher than the warning value (the soft shutdown threshold), a second temperature alert is sent to configured remote alert recipients, and the server begins the shutdown process with an orderly operating-system shutdown. The server then turns itself off. You must select the **Temperature** check box on the Alerts page for the alert to be sent.

   Hard Shutdown
   When the temperature reaches a specified value higher than the soft shutdown value (the hard shutdown threshold), the server immediately shuts down and sends an alert to configured remote alert recipients. You must select the **Temperature** check box on the Alerts page for the alert to be sent.

Note: The hard shutdown alert is sent only if a soft shutdown alert has not yet been sent.

If the system is monitored by a baseboard management controller (BMC) instead of the Remote Supervisor Adapter II, the IPMI thresholds that are supported by the BMC are displayed on the Temperature Thresholds page. The Remote Supervisor Adapter II generates an event when the threshold is reached. The BMC generates any shutdown actions, if they are required.

Non-critical
If the BMC indicates that this threshold has been reached, a warning event is generated.

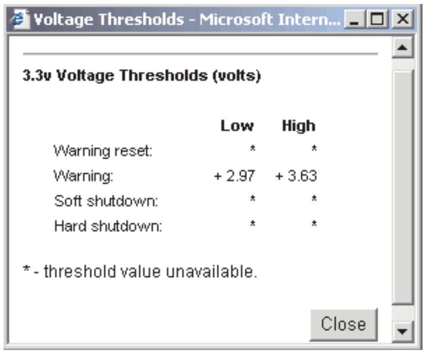
Critical
If the BMC indicates that this threshold has been reached, a critical event is generated.

Non-recoverable
If the BMC indicates that this threshold has been reached, a critical event is generated.

Return to normal
If the BMC indicates that the value has exceeded any of the three thresholds and then dropped below this value, any active events are cleared.

4. Scroll down to the **Voltages** area. The Remote Supervisor Adapter II will send an alert if any monitored power source voltage falls outside its specified operational ranges.

   If you click a voltage reading, a window similar to the one in the following illustration opens.



3.3v Voltage Thresholds (volts)

	Low	High
Warning reset:	*	*
Warning:	+ 2.97	+ 3.63
Soft shutdown:	*	*
Hard shutdown:	*	*

* - threshold value unavailable.

The Voltage Thresholds page displays the voltage ranges at which the Remote Supervisor Adapter II reacts. The voltage threshold values are preset on the remote server and cannot be changed.

The Remote Supervisor Adapter II Web interface displays the voltage readings of the system board and the voltage regulator modules (VRM). The system sets a voltage range at which the following actions are taken:

Warning Reset
When the voltage drops below or exceeds the warning voltage range and then recovers to that range, the server assumes that the voltage has returned to normal, and no further alerts are generated.

Warning
When the voltage drops below or exceeds a specified voltage range, a voltage alert is sent to configured remote alert recipients. You must select the **Voltage** check box on the Alerts page for the alert to be sent.

Soft Shutdown

When the voltage drops below or exceeds a specified voltage range, a voltage alert is sent to configured remote alert recipients, and the server begins the shutdown process with an orderly operating-system shutdown. The server then turns itself off. You must select the **Voltage** check box on the Alerts page for the alert to be sent.

Hard Shutdown

When the voltage drops below or exceeds a specified voltage range, the server immediately shuts down and sends an alert to configured remote alert recipients. You must select the **Voltage** check box on the Alerts page for the alert to be sent.

Note: The hard shutdown alert is sent only if a soft shutdown alert has not yet been sent.

If the system is monitored by a BMC instead of the Remote Supervisor Adapter II, the IPMI thresholds that are supported by the BMC are displayed on the Voltage Thresholds page. The Remote Supervisor Adapter II generates an event when the threshold is reached. The BMC generates any shutdown actions, if they are required.

Non-critical

If the BMC indicates that this threshold has been reached, a warning event is generated.

Critical

If the BMC indicates that this threshold has been reached, a critical event is generated.

Non-recoverable

If the BMC indicates that this threshold has been reached, a critical event is generated.

Return to normal

If the BMC indicates that the value has exceeded any of the three thresholds and then dropped below this value, any active events are cleared.

5. Scroll down to the **Fan Speeds** area. The Remote Supervisor Adapter II Web interface displays the running speed of the server fans (expressed in a percentage of the maximum fan speed). You receive a fan alert (Multiple Fan Failure or Single Fan Failure) when the fan speeds drop to an unacceptable level or the fans stop. You must select the **Fan** check box on the Alerts page for the alert to be sent.
6. Scroll down to the **Display Latest OS Failure Screen** area. Click **View OS Failure Screen** to access an image of the operating-system-failure screen that was captured when the server stopped functioning.

   Notes:

   a. To capture operating-system-failure screens, you must enable the OS Watchdog feature as described in “Setting server timeouts” on page 13.

   b. The operating-system-failure screen capture is available only if a supported operating system is installed on the server.

   If an operating-system-failure screen event occurs while the operating system is running but then the server operating system stops running, the operating-system timeout is triggered, which causes the Remote Supervisor Adapter II to capture the operating-system-failure screen data and store it. The operating-system-failure screen image shows the date and time of the capture. The image will not be overwritten during the next operating-system installation because the Remote Supervisor Adapter II does not capture the operating-system loader screen. Only error conditions are captured and maintained. The Remote Supervisor Adapter II stores only the most recent error event information, overwriting older information when a new error event occurs.

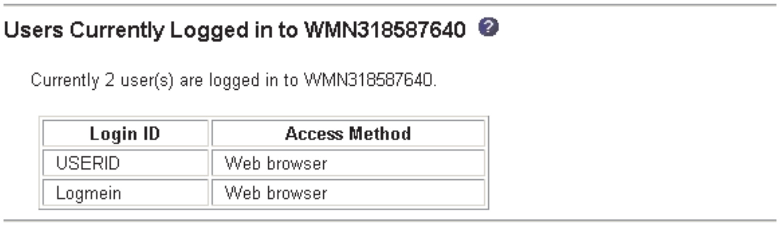
To remotely access a server operating-system-failure screen image, complete the following steps:

a. Log in to the Remote Supervisor Adapter. For more information, see Chapter 2, "Opening and using the Web interface," on page 5.

b. In the navigation pane, click **System Health**, and then scroll down to the **Display Latest OS Failure Screen** area.

c. Click **View OS Failure Screen**. The operating-system-failure screen image is displayed on your screen.

7. Scroll down to the **Users Currently Logged in** area. The Remote Supervisor Adapter II Web interface displays the login ID and access method of each user logged in to the Remote Supervisor Adapter II.

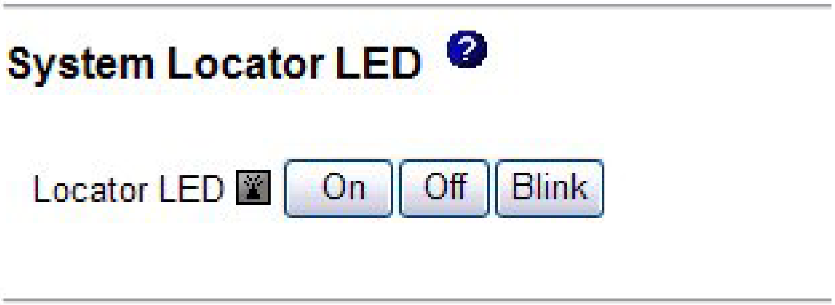


Users Currently Logged in to WMN318587640

Currently 2 user(s) are logged in to WMN318587640.

Login ID	Access Method
USERID	Web browser
Logmein	Web browser

8. Scroll down to the **System Locator LED** area. The Remote Supervisor Adapter II Web interface displays the status of the System Locator LED. It also provides buttons to change the state of the LED. For the meaning of the graphics that are displayed in this area, see the online help.



Viewing the event log

The Event Log page contains all entries that are currently stored in the server event log and POST event log of the remote managed server. Information about all remote access attempts is recorded in the Remote Supervisor Adapter II event log. You can view the event log for all of the servers on an ASM interconnect network. The Remote Supervisor Adapter II time stamps all events and logs them into the event log, sending out the following alerts, if configured to do so by the system administrator:

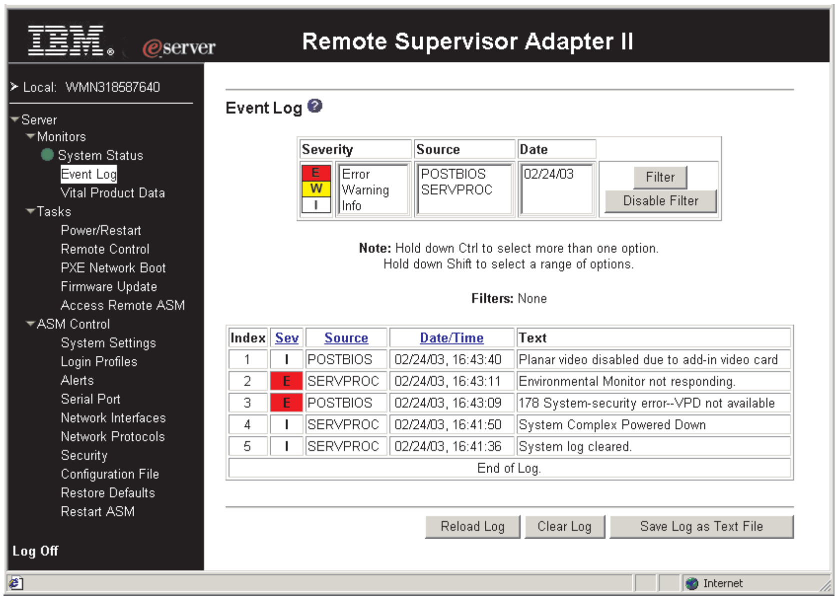
- Event log 75% full
- Event log full

The event log has a limited capacity. When that limit is reached, the older events are deleted in a first-in, first-out order.

You can sort and filter entries in the event log.

To access and view the event log, complete the following steps:

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Event Log** to view the recent history of events on the server. A page similar to the one in the following illustration is displayed.



Event Log

Severity		Source	Date	
E W I	Error Warning Info	POSTBIOS SERVPROC	02/24/03	Filter Disable Filter

Note: Hold down Ctrl to select more than one option.
Hold down Shift to select a range of options.

Filters: None

Index	Sev	Source	Date/Time	Text
1	I	POSTBIOS	02/24/03, 16:43:40	Planar video disabled due to add-in video card
2	E	SERVPROC	02/24/03, 16:43:11	Environmental Monitor not responding.
3	E	POSTBIOS	02/24/03, 16:43:09	178 System-security error--VPD not available
4	I	SERVPROC	02/24/03, 16:41:50	System Complex Powered Down
5	I	SERVPROC	02/24/03, 16:41:36	System log cleared.
End of Log.				

Reload Log · Clear Log · Save Log as Text File

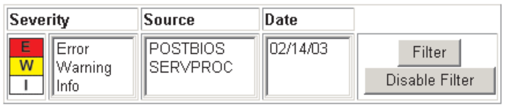
3. Scroll down to view the complete contents of the event log. The events are given the following levels of severity:

   Informational
   This severity level is assigned to an event of which you should take note.

   Warning
   This severity level is assigned to an event that could affect server performance.

   Error This severity level is assigned to an event that needs immediate attention.

   The Remote Supervisor Adapter II Web interface distinguishes warning events with the letter W on a yellow background in the severity column and error events with the letter E on a red background.



Severity		Source	Date	
E W I	Error Warning Info	POSTBIOS SERVPROC	02/14/03	Filter Disable Filter

4. Click **Save Log as Text File** to save the contents of the event log as a text file. Click **Reload Log** to refresh the display of the event log. Click **Clear Log** to delete the contents of the event log.

Viewing vital product data

When the server starts, the Remote Supervisor Adapter II collects system, basic input/output (BIOS) information, and server component vital product data (VPD) and stores it in nonvolatile memory. You can access this information at any time from almost any computer. The Vital Product Data page contains key information about the remote managed server that the Remote Supervisor Adapter II is monitoring.

To view the server component vital product data, complete the following steps:

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Vital Product Data** to view the status of the hardware and software components on the server.
3. Scroll down to view the following VPD readings:

   Machine level VPD
   The vital product data for the server appears in this area. For viewing VPD, the machine-level VPD includes a universal unique identifier (UUID).

   Note: The machine-level VPD, component-level VPD, and component activity log provide information only when the server is turned on.

Table 11. Machine-level vital product data

Field	Function
Machine type	Identifies the type of server that the Remote Supervisor Adapter II is monitoring.
Machine model	Identifies the model number of the server that the Remote Supervisor Adapter II is monitoring.
Serial number	Identifies the serial number of the server that the Remote Supervisor Adapter II is monitoring.
UUID	Identifies the universal unique identifier (UUID), a 32-digit hexadecimal number, of the server that the Remote Supervisor Adapter II is monitoring.

   Component level VPD
   The vital product data for the components of the remote managed server appears in this area.

Table 12. Component-level vital product data

Field	Function
FRU number	Identifies the field replaceable unit (FRU) number (a seven-digit alphanumeric identifier) for each component.
Serial number	Identifies the serial number of each component.
Mfg ID	Identifies the manufacturer ID for each component.
Slot	Identifies the slot number where the component is located.

   Component Activity Log
   You can view a record of component activity in this area.

Table 13. Component activity log

Field	Function
FRU number	Identifies the field replaceable unit (FRU) number (a seven-digit alphanumeric identifier) of the component.
Serial number	Identifies the serial number of the component.
Manufacturer ID	Identifies the manufacturer of the component.
Slot	Identifies the slot number where the component is located.
Action	Identifies the action taken by each component.
Timestamp	Identifies the date and time of the component action. The date is displayed in the *mm/dd/yy* format. The time is displayed in the *hh:mm:ss* format.

In addition, the component activity log tracks the following server components:

- Power supplies
- DIMMs
- Microprocessors (CPUs)
- System board
- Power backplane

POST/BIOS VPD

You can view the power-on self-test (POST) or basic input/output system (BIOS) firmware code VPD for the remote managed server in this area.

Table 14. POST/BIOS vital product data

Field	Function
Version	Indicates the version number of the POST/BIOS code.
Build level	Indicates the level of the POST/BIOS code.
Build date	Indicates when the POST/BIOS code was built.

Diagnostics VPD

You can view the diagnostic code VPD for the remote managed server in this area.

Table 15. Diagnostics vital product data

Field	Function
Version	Indicates the version number of the diagnostic code.
Build level	Indicates the level of the diagnostic code.
Build date	Indicates when the diagnostic code was built.

ASM VPD

You can view vital product data for the Remote Supervisor Adapter II in this area.

Table 16. ASM vital product data

Field	Function
Firmware type	Identifies the ASM firmware component type: main application, boot ROM, video BIOS or device driver.

Table 16. ASM vital product data (continued)

Field	Function
Build ID	Identifies the build IDs of the application firmware and the startup ROM firmware.
File name	Identifies the file names of the application firmware and the startup ROM firmware.
Release date	Identifies the release dates of the application firmware and the startup ROM firmware.
Revision	Identifies the revision numbers of the application firmware and the startup ROM firmware.

Integrated system management processor VPD

You can view the vital product data for the integrated system management processor (ISMP) firmware code in this area.

Table 17. Integrated system management processor vital product data

Field	Function
Firmware revision	Identifies the revision number of the integrated system management processor firmware.

Chapter 5. Performing Remote Supervisor Adapter II tasks

Use the functions under the **Tasks** heading in the navigation pane to directly control the actions of the Remote Supervisor Adapter II and your server. The tasks that you can perform depend on the server in which the Remote Supervisor Adapter II is installed.

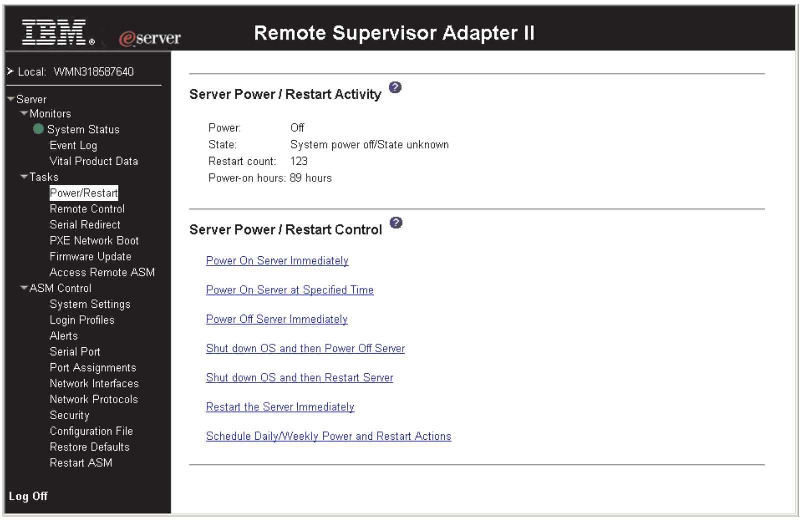
You can perform the following tasks:

- View server power and restart activity
- Remotely control the power status of the server
- Remotely access the server console
- Remotely attach a disk or disk image to the server
- Update the Remote Supervisor Adapter II firmware
- Access other Remote Supervisor Adapter IIs and Remote Supervisor Adapters

Note: Some features are available only on servers running a supported Microsoft Windows operating system.

Server power and restart activity

The **Server Power/Restart Activity** area displays the power status of the server when the Web page was generated.



Server Power / Restart Activity

Power: Off
State: System power off/State unknown
Restart count: 123
Power-on hours: 89 hours

Server Power / Restart Control

Power On Server Immediately
Power On Server at Specified Time
Power Off Server Immediately
Shut down OS and then Power Off Server
Shut down OS and then Restart Server
Restart the Server Immediately
Schedule Daily/Weekly Power and Restart Actions

Power The **Power** field shows the power status of the server at the time this Web page was generated.

State The **State** field shows the state of the server when the Web page was generated. The following states are possible:

- System power off/State unknown
- System in POST
- System stopped in POST (Error detected)
- Booted Flash or System partition
- Booting OS or in unsupported OS (could be in the operating system if the operating system or application does not report the new system state)

- OS booted
- CPUs held in reset

Restart count
The **Restart count** field shows the number of times that the server has been restarted.

Note: The counter is reset to zero each time the ASM subsystem is cleared to factory defaults.

Power-on hours
The **Power-on hours** field shows the total number of hours that the server has been turned on.

Remotely controlling the power status of a server

The Remote Supervisor Adapter II provides full remote power control over your server with power-on, power-off, and restart actions. In addition, power-on and restart statistics are captured and displayed to show server hardware availability.

Attention: Read the following information to prevent the loss of data or damage to data when you perform a remote shutdown of your operating system:

- If the Microsoft Windows 2000, Windows Server 2003, Red Hat Linux, SUSE Linux, or Novell NetWare operating system is installed on your server, you to install the Remote Supervisor Adapter II software to support remote operating system shutdown.
- In the **Power off delay** field, if the value is less than 45 seconds, the Remote Supervisor Adapter II software will adjust the value to 45 seconds when it is loaded. You can decrease the power-off delay value after the server has started, but the Remote Supervisor Adapter II software will reset it to 45 seconds on the next server restart. The Remote Supervisor Adapter II software will not change a power-off delay value that is 45 seconds or greater.

To perform the actions in the **Server Power/Restart Control** area, you must have read/write access to the Remote Supervisor Adapter II. For the operating system shutdown options, the Remote Supervisor Adapter II communicates with the system-management software through the Remote Supervisor Adapter II software, and the system-management software initiates the shutdown.

To perform server power and restart actions, complete the following steps.

Note: Select the following options only in case of an emergency, or if you are offsite and the server is nonresponsive.

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Power/Restart**. Scroll down to the **Server Power/Restart Control** area.
3. Click one of the following options:

Power on server immediately
To turn on the server and start the operating system, click **Power On Server Immediately**.

Power on server at specified time
To turn on the server at a specified time and start the operating system, click **Power on Server at Specified Time** and set the time to turn on the server.

Power off server immediately
To turn off the server without shutting down the operating system, click **Power Off Server Immediately**.

Shut down OS and then power off server
To shut down the operating system and then turn off the server, click **Shutdown OS and then Power Off Server**. This option requires that the Remote Supervisor Adapter II software be installed. You might also have to install IBM Director Agent.

Shut down OS and then restart server
To restart the operating system, click **Shut down OS and then Restart Server**. This option requires that the Remote Supervisor Adapter II software be installed. You might also have to install IBM Director Agent.

Restart the server immediately
To turn off and then turn on the server immediately without first shutting down the operating system, click **Restart the Server Immediately**.

Schedule Daily/Weekly Power and Restart Actions
To shut down the operating system, turn off the server at a specified daily or weekly time (with or without restarting the server), and turn on the server at a specified daily or weekly time, click **Schedule Daily/Weekly Power and Restart Actions**.

A confirmation message is displayed if you select any of these options, and you can cancel the operation if it was selected accidentally.

Remote control

When you use the remote control function, you can view and interact with the server console, and you can assign to the server a CD-ROM drive, diskette drive, or disk image that is on your computer.

You must log in to the Remote Supervisor Adapter II with a user ID that has read/write access to use any of the remote control features.

Important information about updating your Remote Supervisor Adapter II firmware

Important: If you have updated the Remote Supervisor Adapter II firmware to the latest level or plan to in the future, read the following information.

The Remote Supervisor Adapter II uses a Java applet to perform many functions. When the Remote Supervisor Adapter II is updated to the latest firmware level, the Java applet is also updated to the latest level. By default, Java caches (stores locally) applets that were previously used. After a flash update of the Remote Supervisor Adapter II firmware, the Java applet that the server uses might not be at the latest level.

To correct this problem, complete the following steps:

1. Click **Start → Settings → Control Panel**.
2. Double-click **Java Plug-in 1.4**. The Java Plug-in Control Panel window opens.

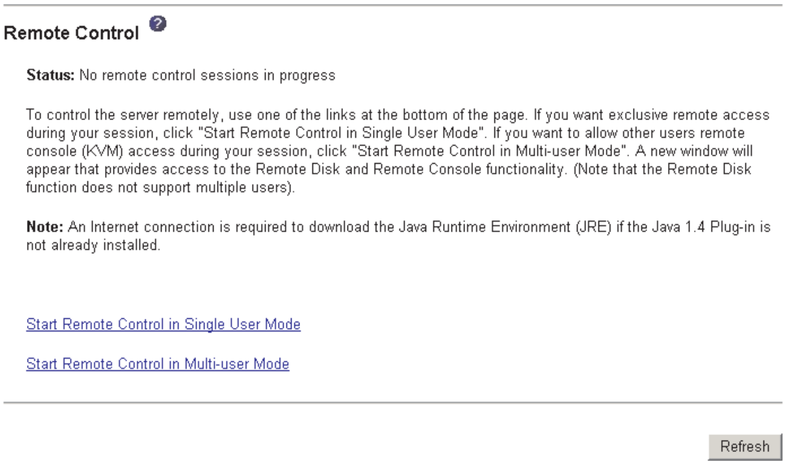
3. Click the **Cache** tab.
4. Choose one of the following options:
   - Clear the **Enable Caching** check box. If you choose this option, Java caching is always disabled.
   - Click **Clear Caching**. If you choose this option, you must click **Clear Caching** after each Remote Supervisor Adapter II firmware update.

Remote console

A remote console is an interactive graphical user interface (GUI) display of the server, viewed on your computer. You see on your monitor exactly what is on the server console, and you have keyboard and mouse control of the console.

To remotely access a server console, complete the following steps:

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Remote Control**. A page similar to the one in the following illustration is displayed.



Remote Control

Status: No remote control sessions in progress

To control the server remotely, use one of the links at the bottom of the page. If you want exclusive remote access during your session, click "Start Remote Control in Single User Mode". If you want to allow other users remote console (KVM) access during your session, click "Start Remote Control in Multi-user Mode". A new window will appear that provides access to the Remote Disk and Remote Console functionality. (Note that the Remote Disk function does not support multiple users).

Note: An Internet connection is required to download the Java Runtime Environment (JRE) if the Java 1.4 Plug-in is not already installed.

Start Remote Control in Single User Mode

Start Remote Control in Multi-user Mode

3. To control the server remotely, use one of the links at the bottom of the Remote Control page. If you want exclusive remote access during your session, click **Start Remote Control in Single User Mode**. If you want to allow other users remote console (KVM) access during your session, click **Start Remote Control in Multi-user Mode**. A new window will open that provides access to the Remote Disk and Remote Console functionality.

   Note: The Remote Disk function does not support multiple users.

You can close the Remote Control window to disconnect from viewing the server console.

Notes:

1. Do not close the Remote Control window if a remote disk is currently mounted. See step 7 on page 85 for instructions for closing and unmounting a remote disk.
2. If you have mouse or keyboard problems when using Remote Control, see the help that is available from the Remote Control page in the Web interface.
3. If you use the remote console to change settings for the Remote Supervisor Adapter II in the server Configuration/Setup Utility program (**Advanced Setup → RSA II Settings**), the server restarts the adapter and you lose the remote

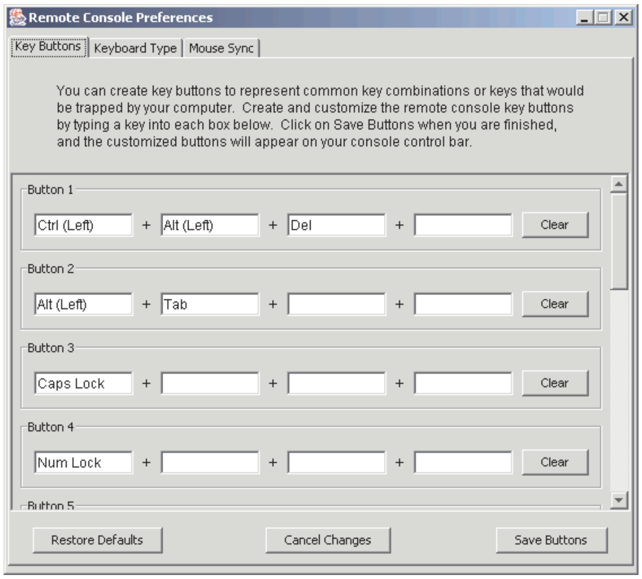
console and the login session. After a short delay, you can log in to the adapter again with a new session, start the remote console again, and exit the server Configuration/Setup Utility program.

Remote console keyboard support

The operating system on the client system that you are using will trap certain key combinations, such as Ctrl+Alt+Del in Microsoft Windows, instead of transmitting them to the server. Other keys, such as F1, might cause an action on your computer as well as on the server. Use the Remote Console **Preferences** link to create and edit customized buttons that can be used to send key strokes to the server.

To create and edit customized buttons, complete the following steps:

1. In the Remote Disk area, click **Preferences**.
2. Click the **Key Button** tab. A window similar to the one in the following illustration opens.



You can create key buttons to represent common key combinations or keys that would be trapped by your computer. Create and customize the remote console key buttons by typing a key into each box below. Click on Save Buttons when you are finished, and the customized buttons will appear on your console control bar.

Button 1: Ctrl (Left) + Alt (Left) + Del +

Button 2: Alt (Left) + Tab + +

Button 3: Caps Lock + + +

Button 4: Num Lock + + +

Button 5

3. Follow the instructions on the Key Button page and the other pages.
4. Click **Save Buttons**.

Remote disk

From the Remote Control window, you can assign to the server a CD-ROM drive or diskette drive that is on your computer, or you can specify a disk image on your computer for the server to use. You can use the drive for functions such as restarting (booting) the server, updating BIOS code or diagnostics code, installing new software on the server, and installing or updating the operating system on the server. You can use the Remote Console function to access the remote disk. The drive will appear as a USB drive on the server.

Notes:

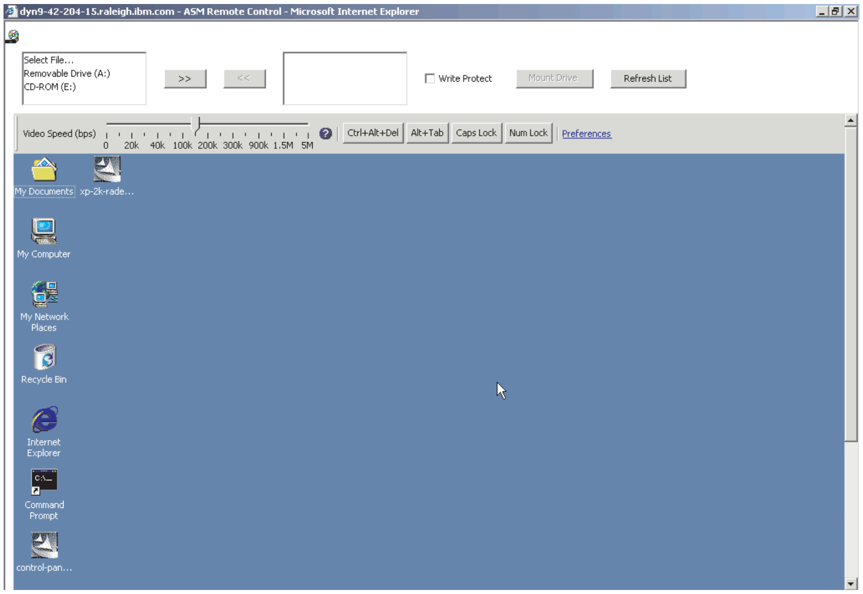
1. The following server operating systems have USB support, which is required for the Remote Disk feature:
   - Microsoft Windows Server 2003
   - Microsoft Windows 2000 with Service Pack 4 or later
   - Red Hat Linux version 7.3

- SUSE Linux version 8.0
- Novell NetWare 6.5

2. The client system requires Microsoft Windows 2000 or later and the Java 1.4 Plug-in or later.
3. The client system must have an Intel® Pentium® III microprocessor or greater, operating at 700 MHz or faster, or equivalent.
4. If the optical drive that is being used on the client system cannot be mounted or read successfully, retry the operation from a different client system. Some client optical drives might not work with the remote disk feature.

To assign a disk drive or disk image on your computer to the server, complete the following steps:

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Remote Control**.
3. In the Remote Control page, click one of the **Start Remote Control** options. A page similar to the one in the following illustration is displayed.



The Remote Control window contains the remote disk controls in the **Remote Disk** area at the top of the window. The Remote Control window also contains the server console in the **Remote Console** area (see “Remote console” on page 82).

4. To mount hard disk drives or disk images on the server, select the hard disk drives or images in the left side of the Remote Disk drive selector, and use the **>>** button to move them to the right side. Use the **<<** button to remove items from the right side. When you click **Mount Drives**, the drives or images that are shown in the right side will be mounted. Before mounting, select the **Write Protect** check box to prevent data from being written to the mounted drives.

   When you select a diskette drive or an image file and move it to the right side of the drive selector, you have the option to save the disk image in the Remote Supervisor Adapter II random access memory (RAM). This enables the disk image to remain mounted on the server so that you can access the disk image later, even after the Web interface session is terminated. All other mounted drives will be unmounted when the Remote Control window is closed. A maximum of one drive or image can be stored on the Remote Supervisor Adapter II. The size of the drive or image contents must be 1.44 MB or smaller.

Important: You will lose the disk image when the Remote Supervisor Adapter II is restarted or the Remote Supervisor Adapter II firmware is updated.

If the **Encrypt disk and KVM data during transmission** check box was selected before the Remote Control window was opened, the disk data is encrypted with 3DES encryption.

Note: The **Encrypt disk and KVM date during transmission** check box is not available on all servers.

To use the mounted disk, use the Remote Console function. The mounted disk will appear as a USB disk drive that is attached to the server.

5. In the drop-down list in the **Remote Disk** area of the Remote Control window, click the item that you want. The choices are listed by the type of drive, followed by the volume label.

   Select File
   A disk image on your computer.

   Removable Drive
   A diskette drive on your computer.

   CD-ROM
   A CD drive on your computer.

   USB flash drive
   A portable, solid-state storage device that usually uses flash memory on your computer.

   Consider the following guidelines:

   - As of the date of this document, USB flash drives are supported only on clients running Microsoft Windows.
   - A USB flash drive is shown as a removable drive in the remote control window.
   - After the drive is mounted, it can be used for read or write operations and for starting the server from the drive.
   - When you copy files to the flash drive, you must type the `sync` command (for Linux) or click the **Safely remove device** icon (for Windows) to complete the write process.

     Do *not* access the device locally (for example, viewing the files locally on the client side) until you have removed and reinserted the USB flash drive.

6. Click **Mount Drive**. If you clicked **Select File** in step 5, browse to select the disk image file to use.

   The drive or disk image will function as a USB device that is connected to the server.

   To refresh the list of available drives on your computer, click **Refresh List** in the Remote Control window.

7. When you have finished using the drive or disk image, close and unmount it. For Microsoft Windows, to close and unmount the drive or drive image, complete the following steps:

   a. Double-click the **Unplug or Eject Hardware** icon in the Windows taskbar at the bottom right of the screen. If there is no icon, complete the following steps:

1) In the Microsoft Windows Control Panel, click **Add/Remove Hardware**; then, click **Next**.
2) Select **Uninstall/Unplug a device**; then, click **Next**.
3) Click **Unplug/Eject a device**; then, click **Next**.

b. Select **USB Mass Storage Device** and click **Stop**.

c. Click **Close**.

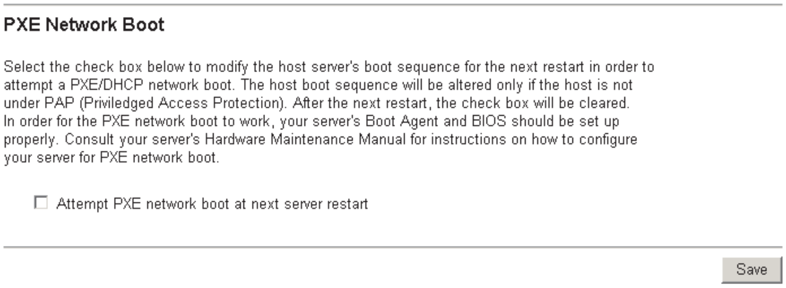
d. In the Remote Control window, click **Unmount Drive**.

Setting up PXE network boot

Note: The PXE network boot feature is not available on all servers.

Complete the following steps to set up your server to attempt a Preboot Execution Environment (PXE) network boot at the next server restart:

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **PXE Network Boot**. A page similar to the one in the following illustration is displayed.



PXE Network Boot

Select the check box below to modify the host server's boot sequence for the next restart in order to attempt a PXE/DHCP network boot. The host boot sequence will be altered only if the host is not under PAP (Priviledged Access Protection). After the next restart, the check box will be cleared. In order for the PXE network boot to work, your server's Boot Agent and BIOS should be set up properly. Consult your server's Hardware Maintenance Manual for instructions on how to configure your server for PXE network boot.

□ Attempt PXE network boot at next server restart

3. Select the **Attempt PXE network boot at next server restart** check box.
4. Click **Save**.

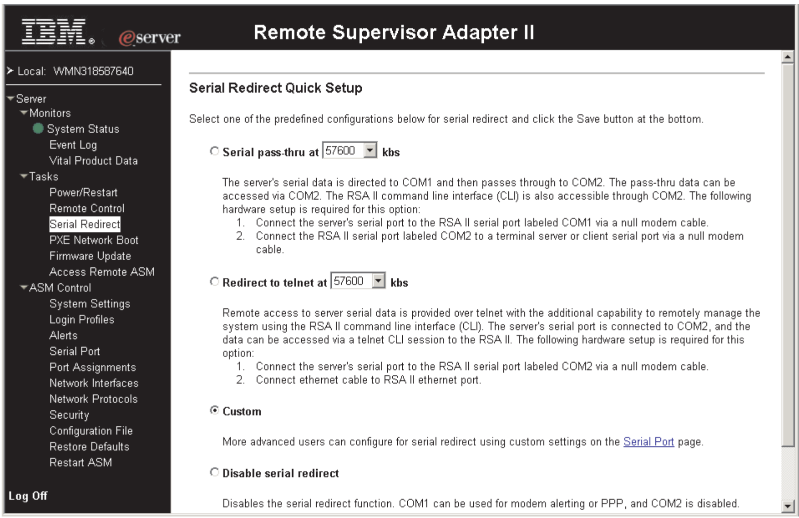
Serial redirection quick setup

Note: This feature is not available on the Remote Supervisor Adapter II SlimLine in some servers.

You can use the Remote Supervisor Adapter II Web interface serial redirection wizard to simplify the configuration of serial redirection.

To use the serial redirection wizard, complete the following steps:

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Serial Redirect**. A page similar to the one in the following illustration is displayed.



Serial Redirect Quick Setup

Select one of the predefined configurations below for serial redirect and click the Save button at the bottom.

○ **Serial pass-thru at** 57600 **kbs**

The server's serial data is directed to COM1 and then passes through to COM2. The pass-thru data can be accessed via COM2. The RSA II command line interface (CLI) is also accessible through COM2. The following hardware setup is required for this option:

1. Connect the server's serial port to the RSA II serial port labeled COM1 via a null modem cable.
2. Connect the RSA II serial port labeled COM2 to a terminal server or client serial port via a null modem cable.

○ **Redirect to telnet at** 57600 **kbs**

Remote access to server serial data is provided over telnet with the additional capability to remotely manage the system using the RSA II command line interface (CLI). The server's serial port is connected to COM2, and the data can be accessed via a telnet CLI session to the RSA II. The following hardware setup is required for this option:

1. Connect the server's serial port to the RSA II serial port labeled COM2 via a null modem cable.
2. Connect ethernet cable to RSA II ethernet port.

● **Custom**

More advanced users can configure for serial redirect using custom settings on the Serial Port page.

○ **Disable serial redirect**

Disables the serial redirect function. COM1 can be used for modem alerting or PPP, and COM2 is disabled.

3. Use the following information to complete the quick setup information:

Serial pass-thru

The serial data of the server is directed to COM1 and then passes through to COM2. The pass-thru data can be accessed through COM2. The Remote Supervisor Adapter II command line interface (CLI) is also accessible through COM2. The following hardware setup is required for this option:

- Connect the serial port of your server to the Remote Supervisor Adapter II serial port that is labeled “COM1” by using a null modem cable.
- Connect the Remote Supervisor Adapter II serial port that is labeled “COM2” to a terminal server or client serial port by using a null modem cable.

Redirect to Telnet

Remote access to server serial data is provided over Telnet with the additional capability to remotely manage the system by using the Remote Supervisor Adapter II command line interface (CLI). The server serial port is connected to COM2, and you can access the data by using a Telnet CLI session to the Remote Supervisor Adapter II. The following hardware setup is required for this option:

- Connect the server serial port to the Remote Supervisor Adapter II serial port that is labeled “COM2” by using a null modem cable.
- Connect an Ethernet cable to the Remote Supervisor Adapter II Ethernet port.

Custom

Advanced users can configure for serial redirection by using custom settings on the Serial Port page. To access the Serial Port settings page, click **Serial Port**.

Disable serial redirect

This option disables the serial redirect function. COM1 can be used for modem alerting or PPP, and COM2 is disabled.

Updating firmware

Use the Firmware Update option on the navigation pane to update the firmware of the Remote Supervisor Adapter II.

Notes:

1. To remotely update the firmware or operating system on the server, see "Remote disk" on page 83.
2. If you plan to use the Remote Control feature after you update the firmware, see "Important information about updating your Remote Supervisor Adapter II firmware" on page 81.

To update the startup or main application files of the Remote Supervisor Adapter II, complete the following steps:

1. Download the latest firmware update applicable for the server in which the Remote Supervisor Adapter II is installed.
   a. Go to http://www.ibm.com/support/.
   b. Under **Support topics**, select **Multiple file download for personal computing**.
   c. In the "Downloads and drivers" window, under **Select a product**, in the **Brand** field, select Servers.
   d. In the **Family** field, select the server in which the Remote Supervisor Adapter II is installed.
   e. Click **Continue**.
   f. Scroll to the **Remote Supervisor Adapter II** area and select the link for the firmware update.
2. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, "Opening and using the Web interface," on page 5.
3. In the navigation pane, click **Firmware Update**.
4. Click **Browse**.
5. Navigate to the PKT or PKC file that you want to update.

   Note: For most firmware updates, you are required to update only the Boot Record and Main Application packets.
6. Click **Open**.

   The file (including the full path) is displayed in the box beside **Browse**.
7. To begin the update process, click **Update**.

   A progress indicator opens as the file is transferred to temporary storage on the Remote Supervisor Adapter II. A confirmation window opens when the file transfer is completed.
8. Verify that the PKT or PKC file that is shown on the Confirm Firmware Update window is what you intend to update. If it is not, click **Cancel**.
9. To complete the update process, click **Continue**.

   A progress indicator opens as the firmware on the Remote Supervisor Adapter II is flashed. A confirmation window opens to verify that the update was successful.
10. In the navigation pane, click **Restart ASM** and then click **Restart**.

    Note: You must restart the Remote Supervisor Adapter II after each firmware packet is successfully updated.
11. Click **OK** to confirm that you want to restart the Remote Supervisor Adapter II.

12. Click **OK** to close the current browser window.
13. Repeat step 2 on page 88 through step 12 for each packet that you must update.
14. After the Remote Supervisor Adapter II firmware is updated, log in to the Remote Supervisor Adapter II again to access the Web interface.

Accessing remote adapters through an ASM interconnect network

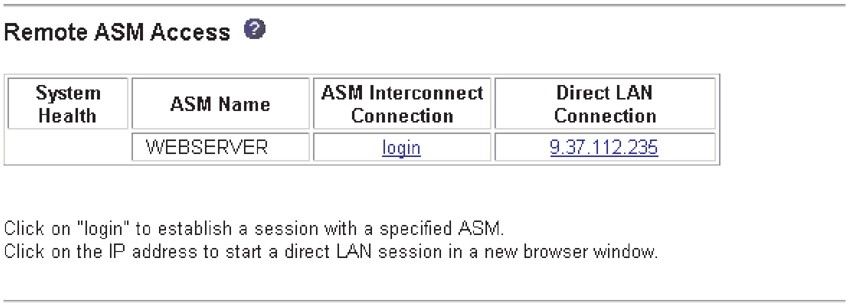
Note: This feature is not available on the Remote Supervisor Adapter II SlimLine.

You can connect to remote systems through the ASM interconnect network from the Access Remote ASM link. The Remote ASM Access table displays color-coded icons to indicate the overall status of each remote system in the System Health column. The system name is the name that corresponds to each remote system. The ASM Interconnect Connection column provides a login link that you can use to quickly access each remote system.

Note: Although it is possible to access a Remote Supervisor Adapter II from a server that is using a Remote Supervisor Adapter, doing so does not present the full function of a Remote Supervisor Adapter II. Log in to the Remote Supervisor Adapter II first and then log in to the Remote Supervisor Adapter to obtain full Remote Supervisor Adapter II functionality.

To access a Remote Supervisor Adapter, a Remote Supervisor Adapter II, an ASM PCI adapter, or an ASM processor on the ASM interconnect network, complete the following steps:

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, “Opening and using the Web interface,” on page 5.
2. In the navigation pane, click **Access Remote ASM**. A page similar to the one in the following illustration is displayed.



Remote ASM Access

System Health	ASM Name	ASM Interconnect Connection	Direct LAN Connection
	WEBSERVER	login	9.37.112.235

Click on "login" to establish a session with a specified ASM.
Click on the IP address to start a direct LAN session in a new browser window.

3. The Remote ASM Access page contains a table that lists processors and adapters that are linked to the host server. The table also displays the following information:

   System Health
   The system health icon of the remote service processor is displayed in this column.

   ASM Name
   The name of the remote service processor is displayed in this column.

   ASM Interconnect Connection
   The ASM Interconnect Connection column provides a login link that you can use to quickly access each remote system through the ASM interconnect network. To log in to a remote system that is displayed in

the table, click the login link that corresponds to the remote system that you want to access. Then, follow the standard login procedure to gain access to that system.

Direct LAN Connection

Click the IP address link to bypass the ASM interconnect connection and to connect to a remote system directly through your Ethernet network. This connection offers faster access to a remote ASM.

To directly log in to a remote system that is displayed in the table, click the IP address link that corresponds to the remote system that you want to access. Then, follow the standard login procedure to gain access to that remote system.

Note: In certain cases, no IP address link for a direct LAN connection will be available, for one of the following reasons:

no LAN support

The service processor of the remote system does not have access to a LAN port.

function not supported

The service processor of the remote system does not have the ability to report its IP address through the ASM interconnect network.

no LAN connection

The service processor of the remote system has one of the following conditions:

- It has not been manually configured with an IP address.
- It failed to receive a dynamic IP address assignment from a DHCP server.
- It has a faulty physical LAN connection.

4. Click the **login** link that corresponds to the processor or adapter that you want to access under the ASM Interconnect Connection column heading.

   Note: It might take up to 45 seconds for newly attached servers to be reflected in the table of available remote servers, and up to 2 minutes for servers to be removed from the table when they are detached from the ASM interconnect network.

   The Enter Network Password window opens.

5. Type your user name and password and click **OK**. The System Health Summary page is displayed. The adapter or processor name appears in orange above the navigation pane.

   Note: Depending on the service processor that is on the remote server, some options might not be available.

6. Click **Log Off Remote ASM** to log off from the remote server.

Chapter 6. Command-line interface

Use the Remote Supervisor Adapter II command line interface (CLI) to access the Remote Supervisor Adapter II or Remote Supervisor Adapter II SlimLine without having to use the Web interface. It provides a subset of the management functions that are provided by the Web interface.

You can access the CLI through a Telnet session, SSH, or a serial connection. You will be authenticated by the Remote Supervisor Adapter II or Remote Supervisor Adapter II SlimLine before you can issue any CLI commands.

Accessing the command line

You can access the command line using the following methods:

- Start a Telnet or SSH session to the Remote Supervisor Adapter II IP address.
- Connect a null modem cable to the serial port and start a hyperterminal session (not available for the Remote Supervisor Adapter II SlimLine).

Note: You cannot access the command line in-band using the Remote Supervisor Adapter II software.

Logging in to the command-line session

To log into the command line, complete the following steps:

1. Establish a connection with the Remote Supervisor Adapter II.
2. At the user name prompt, type the user ID that you use to log in to the Remote Supervisor Adapter II Web interface.
3. At the password prompt, type the password that you use to log in to the Remote Supervisor Adapter II Web interface.

   You are logged in to the command line. The command-line prompt is the text ID of the Remote Supervisor Adapter II, for example, x345RSA. The command-line session continues until you type `exit` at the command line. Then you are logged off and the session is ended.

Command syntax

Read the following guidelines before using the commands:

- Each command has the following format:

  ```
  command [arguments] [-options]
  ```
- The command syntax is case sensitive.
- The command name is all lowercase.
- All arguments must immediately follow the command. The options immediately follow the arguments.
- Each option is always preceded by a hyphen (-). An option can be a short option (single letter) or a long option (multiple letters).
- If an option has an argument, the argument is mandatory, for example:

  ```
  ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0
  ```

  where **ifconfig** is the command, eth0 is an argument, -i, -g, and -s are options. In this example, all three options have arguments.
- Brackets indicate that an argument or option is optional. Brackets are not part of the command that you type.

Features and limitations

The CLI has the following features and limitations:

- Multiple concurrent CLI sessions are allowed with different access methods (Telnet, SSH, or serial).
  - At most, two Telnet command-line sessions can be active at any time. (The number of Telnet sessions is configurable: valid values are 0,1, and 2, with 0 meaning that the Telnet interface is disabled).
  - At most, two SSH command-line sessions can be active at any time. This number is fixed.
- One command is allowed per line (160-character limit, including spaces).
- There is no continuation character for long commands. The only editing function is the Backspace key to erase the character that you just typed.
- The Up and Down arrow keys can be used to browse through the last eight commands. The **history** command displays a list of the last eight commands, which you can then use as a shortcut to execute a command, as in the following example:

```
x345RSA> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
x345RSA> !0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n ASMA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
x345RSA>
```

- In the command-line interface, the output buffer limit is 2 KB. There is no buffering. The output of an individual command cannot exceed 2048 characters. This limit does not apply in serial redirect mode (the data is buffered during serial redirect).
- The output of a command appears on the screen after the command has completed execution. This makes it impossible for commands to report real-time execution status. For example, in the verbose mode of the **flashing** command, you will not see the flashing progress in real time. You will see it after the command completes execution.
- Simple text messages are used to denote command execution status, as in the following example:

```
x345RSA> power on
ok
x345RSA> power state
Power: On
State: System power off/State unknown
x345RSA>
```

- The command syntax is case sensitive.
- There must be at least one space between an option and its argument. For example, `ifconfig eth0 -i192.168.70.133` is incorrect syntax. The correct syntax is `ifconfig eth0 -i 192.168.70.133`.

- All commands have the `-h`, `-help`, and `?` options, which give syntax help. All of the following examples will give the same result:

  ```
  x345RSA> power -h
  x345RSA> power -help
  x345RSA> power ?
  ```

- Some of the commands listed in the following sections might not be available. To see a list of the commands that are supported, use the help or ? option, as shown in the following examples:

  ```
  x345RSA> help
  x345RSA> ?
  ```

Utility commands

The utility commands are as follows:

- exit
- help
- history

exit command

Description

Use the **exit** command to log off and end the command-line interface session.

help command

Description

Use the **help** command to display a list of all commands with a short description for each. You can also type ? at the command prompt.

history command

Description

Use the **history** command to display an indexed history list of the last eight commands that were issued. The indexes can then be used as shortcuts (preceded by !) to reissue commands from this history list.

Example

```
x345RSA> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
x345RSA> !0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n ASMA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
x345RSA>
```

Monitor commands

The monitor commands are as follows:

- clearlog
- fans
- readlog
- syshealth
- temps
- volts

clearlog command

Description

Use the **clearlog** command to clear the event log of the Remote Supervisor Adapter II or Remote Supervisor Adapter II SlimLine. You must have the authority to clear event logs to use this command.

fans command

Description

Use the **fans** command to display the speed for each of the server fans.

Example

```
x345RSA> fans
fan1 75%
fan2 80%
fan3 90%
x345RSA>
```

readlog command

Syntax

```
readlog [options]
option:
-f
```

Description

Use the **readlog** command to display the ASM event log entries, five at a time. The entries are displayed from the most recent to the oldest.

readlog displays the first five entries in the event log, starting with the most recent, on its first execution, and then the next five for each subsequent call.

readlog -f resets the counter and displays the first 5 entries in the event log, starting with the most recent.

Example

```
x345RSA> readlog -f
1 I SERVPROC 12/18/03 10:18:58 Remote Login Successful.
Login ID:''USERID' CLI authenticated from 192.168.70.231 (Telnet).'
2 I SERVPROC 12/18/03 10:12:22 Remote Login successful.
Login ID: ''USERID' from web browser at IP@=192.168.70.231'
3 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
4 E SERVPROC 12/18/03 10:10:37 Environmental monitor not responding.
5 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
x345RSA> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
```

```
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
being used: 0x00-09-6B-CA-0C-80
x345RSA>
```

syshealth command

Description

Use the **syshealth** command to get a summary of the health of the server. The power state, system state, restart count, and Remote Supervisor Adapter II software status are displayed.

Example

```
x345RSA> syshealth
Power On
State System power off/State unknown
DD not active
Restarts 0
x345RSA>
```

temps command

Description

Use the **temps** command to display all the temperatures and temperature thresholds. The same set of temperatures are displayed as in the Web interface.

Example

```
x345RSA> temps
Temperatures are displayed in degrees Fahrenheit/Celsius
        WR      W      T     SS     HS
----------------------------------------
CPU1   65/18  72/22  80/27  85/29  90/32
CPU2   58/14  72/22  80/27  85/29  9/320
DASD1  66/19  73/23  82/28  88/31  9/332
Amb    59/15  70/21  83/28  90/32  9/355
x345RSA>
```

Notes:

1. The output has the following column headings:

   WR: warning reset

   W: warning

   T: temperature (current value)

   SS: soft shutdown

   HS: hard shutdown
2. All temperature values are in degrees Fahrenheit/Celsius

volts command

Description

Use the **volts** command to display all the voltages and voltage thresholds. The same set of voltages are displayed as in the Web interface.

Example

```
x345RSA> volts
      HSL   SSL   WL    WRL   V     WRH   WH   SSH    HSH
----------------------------------------------------------
5v    5.02  4.00  4.15  4.50  4.60  5.25  5.50  5.75  6.00
```

```
3.3v  3.35  2.80  2.95  3.05  3.10  3.50  3.65  3.70  3.85
12v   12.25 11.10 11.30 11.50 11.85 12.15 12.25 12.40 12.65
-5v   -5.10 -5.85 -5.65 -5.40 -5.20 -4.85 -4.65 -4.40 -4.20
-3.3v -3.35 -4.10 -3.95 -3.65 -3.50 -3.10 -2.95 -2.80 -2.70
VRM1                          3.45
VRM2                          5.45
x345RSA>
```

Note: The output has the following column headings:

HSL: hard shutdown low
SSL: soft shutdown low
WL: warning low
WRL: warning reset low
V: voltage (current value)
WRH: warning reset high
WH: warning high
SSH: soft shutdown high
HSH: hard shutdown high

vpd command

Syntax

```
vpd sys
vpd asm
vpd bios
vpd ismp
vpd exp
```

Description

Use the **vpd** command to display vital product data for the system (sys), Remote Supervisor Adapter II (asm), Remote Supervisor Adapter II SlimLine (asm), system BIOS (bios), ISMP (ismp) and PCI-X expansion boxes (exp). The same information is displayed as in the Web interface.

Example

```
x345RSA> vpd asm
Type   BuildID     Filename         BuildDate   Rev
-----------------------------------------------------
Main   GRE814      GRETMNUS.PKT     12-03-03    16
Boot   GRE814      GRETBTUS.PKT     11-19-03    16
Video  AV234X.1234.789
DD     RE78936
x345RSA> vpd bios
Type   BuildID     BuildDate    Rev
-----------------------------------
BIOS   GRJT09      11-14-03     10
x345RSA>
```

Server power and restart control commands

The server power and restart commands are as follows:

- power
- reset

power command

Syntax

```
power on
power off [-s]
power state
power cycle [-s]
```

Description

Use the **power** command to control the server power. To issue the **power** commands, you must have power and restart access authority.

power on turns on the server power.

power off turns off the server power. The **-s** option shuts down the operating system before the server is turned off.

Note: The Remote Supervisor Adapter II software must be installed and running for the **-s** option to function correctly.

power state displays the server power state (on or off) and the current state of the server.

power cycle turns off the server power and then turns on the power. The **-s** option shuts down the operating system before the server is turned off.

Note: The Remote Supervisor Adapter II software must be installed and running for the **-s** option to function correctly.

reset command

Syntax

```
reset [option]
option:
-s
```

Description

Use the **reset** command to restart the server. To use this command, you must have power and restart access authority. The **-s** option shuts down the operating system before restarting the server. When the **-s** option is specified, the Remote Supervisor Adapter II software state is checked and if it is not active, the server is not restarted. Instead, a message is displayed indicating that the Remote Supervisor Adapter II software is not active.

Serial redirect command

There is one serial redirect command: console.

console command

Note: The **console** command is not available for the Remote Supervisor Adapter II SlimLine.

Syntax

```
console 1
console 2
```

Description

Use the **console** command to start a serial redirect console session to the designated serial port of the Remote Supervisor Adapter II or the Remote Supervisor Adapter II SlimLine.

Configuration commands

The configuration commands are as follows:

- dhcpinfo
- ifconfig
- ldap
- ntp
- passwordcfg
- portcfg
- slp
- srcfg
- ssl
- tcpcmdmode
- timeouts
- users

dhcpinfo command

Syntax

```
dhcpinfo eth0
```

Description

Use the **dhcpinfo** command to view the DHCP server-assigned IP configuration for eth0, if the interface is configured automatically by a DHCP server. You can use the **ifconfig** command to enable or disable DHCP.

Example

```
x345RSA> dhcpinfo eth0
-server 192.168.70.29
-n ASMA00096B9E003A
-i 192.168.70.202
-g 192.168.70.29
-s 255.255.255.0
-d linux-sp.raleigh.ibm.com
-dns1 192.168.70.29
-dns2 0.0.0.0
-dns3 0.0.0.0
x345RSA>
```

The following table describes the output from the example.

Option	Description
-server	DHCP server that assigned the configuration
-n	Assigned host name
-i	Assigned IP address
-g	Assigned gateway address
-s	Assigned subnet mask

Option	Description
-d	Assigned domain name
-dns1	Primary DNS server IP address
-dns2	Secondary DNS IP address
-dns3	Tertiary DNS server IP address

ifconfig command

Syntax

```
ifconfig eth0 [options]
ifconfig ppp [options]
eth0 options:
-state interface_state
-c config_method
-i static_ip_address
-g gateway_address
-s subnet_mask
-n hostname
-r data_rate
-d duplex_mode
-m max_transmission_unit
-l locally_administered_MAC

ppp options:
-state enabled/disabled - interface status
-i ip_addr - IP address
-ri ip_addr - remote IP address
-s ip addr  - subnet mask
-a pap|chap|cthenp  - authentication method
```

Note: The **ifconfig ppp** command is not available for the Remote Supervisor Adapter II SlimLine.

Description

Use the **ifconfig** command to configure the Ethernet interface. Type `ifconfig eth0` to display the current Ethernet interface configuration. To change the Ethernet interface configuration, type the options, followed by the values. To change the interface configuration, you must have at least Adapter Networking and Security Configuration authority.

The following table shows the arguments for the options.

Option	Description	Values
-state	Interface state	disabled, enabled
-c	Configuration method	dhcp, static, dthens (dthens corresponds to the “try dhcp server, if it fails use static config” option on the Web interface)
-i	Static IP address	Valid IP address format
-g	Gateway address	Valid IP address format
-s	Subnet mask	Valid IP address format
-n	Host name	String of up to 63 characters. Can include letters, digits, periods, underscores, and hyphens.
-r	Data rate	10, 100, auto
-d	Duplex mode	full, half, auto

Option	Description	Values
-m	MTU	Numeric between 60 and 1500
-l	LAA	MAC address format. Multicast addresses are not allowed (the first byte must be even).
-ri	Remote IP address	Valid IP address format
-a	Authentication protocol	pap, chap, cthenp

Example

```
x345RSA> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n ASMA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
x345RSA> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the ASM.
x345RSA>
```

Note: The **-b** option in the ifconfig display is for the burned-in MAC address. The burned-in MAC address is read-only and is not configurable.

ldap command

Syntax

```
ldap [options]
options:
   -a loc|ldap|locId|Idloc
   -b anon|client|login
   -c client_dn
   -d search_domain
   -f group_filter
   -g group_search_attr
   -l string
   -m login|cfg|lthenc
   -n service_name
   -p client_pw
   -pc confirm_pw
   -r root_dn
   -s1ip host name/ip_addr
   -s2ip host name/ip_addr
   -s3ip host name/ip_addr
   -s1pn port_number
   -s2pn port_number
   -s3pn port_number
   -u search_attrib
   -v off|on
   -w on|off
   -h
```

Description

Use the **ldap** command to display and configure the LDAP protocol configuration parameters.

The following table shows the arguments for the options.

Option	Description	Values
-a	User authentication method	Local only, LDAP only, local first then LDAP, LDAP first then local
-b	Binding method	Anonymous, bind w/ClientDN and password, user principal bind (UPN)
-c	Client distinguished name	String of up to 63 characters for *client_dn*
-d	Search domain	String of up to 31 characters for *search_domain*
-f	Group filter	String of up to 63 characters for *group_filter*
-g	Group search attribute	String of up to 63 characters for *group_search_attr*
-l	Login permission attribute	String of up to 63 characters for *string*
-m	Domain source	Extract search domain from login ID, use only configured search domain, try login first then configured value
-n	Service name	String of up to 15 characters for *service_name*
-p	Client password	String of up to 15 characters for *client_pw*
-pc	Confirm client password	String of up to 15 characters for *confirm_pw* Command usage is: ldap -p *client_pw* -pc *confirm_pw* This option is required when changing the client password. It compares the *confirm_pw* argument with the *client_pw* argument and the command will fail if they do not match.
-r	Root entry distinguished name (DN)	String of up to 63 characters for *root_dn*
s1ip	Server 1 host name/IP address	String up to 63 characters or an IP address for *host name/ip_addr*
s2ip	Server 2 host name/IP address	String up to 63 characters or an IP address for *host name/ip_addr*
s3ip	Server 3 host name/IP address	String up to 63 characters or an IP address for *host name/ip_addr*
s1pn	Server 1 port number	A numeric port number up to 5 digits for *port_number.*
s2pn	Server 2 port number	A numeric port number up to 5 digits for *port_number.*
s3pn	Server 3 port number	A numeric port number up to 5 digits for *port_number.*
-u	UID search attribute	String of up to 23 characters for *search_attrib*
-v	Get LDAP server address via DNS	Off, on
-w	Allows wildcards in the group name	Off, on
-h	Displays the command usage and options	

ntp command

Syntax

```
ntp [options]
options:
-en state
-i  hostname
-f  frequency
-synch
```

Description

Use the **ntp** command to display and configure the Network Time Protocol (NTP).

The following table shows the arguments for the options.

Option	Description	Values
-en	Enables or disables the Network Time Protocol	Enabled, disabled
-i	Name or IP address of the Network Time Protocol server	The name of the NTP server to be used for clock synchronization.
-f	The frequency (in minutes) that the Remote Supervisor Adapter II clock is synchronized with the Network Time Protocol server	1 to 65535
-synch	Requests an immediate synchronization with the Network Time Protocol server	No values are used with this parameter.

Example

```
x345RSA> ntp
-en: disabled
-f: 1 minute
-i: not set
```

passwordcfg command

Syntax

```
passwordcfg [options]
options: {-high}|{-legacy}|{-exp|-cnt|-nul}
-legacy
-high
-exp:
-cnt:
-nul:
-h
```

Description

Use the **passwordcfg** command to display and configure the password parameters.

Option	Description
-legacy	Sets account security to a predefined legacy set of defaults
-high	Sets account security to a predefined high set of defaults

Option	Description
-exp	Maximum password age [0 - 365] days. Set to 0 for no expiration.
-cnt	Number of previous passwords that cannot be reused [0 - 5]
-nul	Allows accounts with no password [yes	no]
-h	Displays the command usage and options

Example

```
x345RSA> passwordcfg
Security Level: Legacy
x345RSA> passwordcfg -exp 365
ok
x345RSA> passwordcfg -nul yes
ok
x345RSA> passwordcfg -cnt 5
ok
x345RSA> passwordcfg
Security Level: Customize
-exp: 365
-cnt: 5
-nul: allowed
```

portcfg command

Note: The **portcfg** command is not available for the Remote Supervisor Adapter II SlimLine.

Syntax

```
portcfg com1 [options]
portcfg com2 [options]
options:
-serred serial_redirect_mode
-b baud_rate
-p parity
-s stop_bits
-climode cli_mode
-cliauth cli_auth
```

Description

Use the **portcfg** command to configure the serial port. Type `portcfg com1` or `portcfg com2` to display the port configuration. To change the serial port configuration, type the options, followed by the values. To change the serial port configuration, you must have at least Adapter Networking and Security Configuration authority.

The following table shows the arguments for the options.

Option	Description	Values
-serred	Serial redirect mode	disabled, enabled
-b	Baud rate	2400, 4800, 9600, 19200, 38400, 57600, 115200
-p	Parity	none, odd, even, mark, space
-s	Stop bits	1, 2

Option	Description	Values
-climode	CLI mode	none, cliems, cliuser • none: The command-line interface is disabled • cliems: The command-line interface is enabled with EMS-compatible keystroke sequences • cliuser: The command-line interface is enabled with user-defined keystroke sequences
-cliauth	CLI authentication	enabled, disabled

Example

```
x345RSA> portcfg com1
-serred enabled
-b 57600
-p none
-s 1
-climode cliems
-cliauth enabled
x345RSA> portcfg com1 -climode cliuser
ok
x345RSA>
```

slp command

Syntax

```
slp [options]
options:
-t
-i
```

Description

Use the **slp** command to display and configure the Service Location Protocol (SLP) parameters.

Option	Description
-t	SLP address type (multicast/broadcast)
-i	SLP multicast address (must be between 224.0.0.0 and 239.255.255.255)

Example

```
x345/RSA> slp -t multicast
OK
x345/RSA> slp
-t multicast
-i 239.255.255.253
x345/RSA>
```

srcfg command

Note: The **srcfg** command is not available for the Remote Supervisor Adapter II SlimLine.

Syntax

```
srcfg [options]
options:
-passthru passthru_mode
-entercliseq entercli_keyseq
-exitcliseq exitcli_keyseq
```

Description

Use the **srcfg** command to configure the serial redirection. Type `srcfg` to display the current configuration. To change the serial redirect configuration, type the options, followed by the values. To change the serial redirect configuration, you must have at least Adapter Networking and Security Configuration authority.

The following table shows the arguments for the options.

Option	Description	Values
-passthru	Serial passthru	disabled, enabled (this corresponds to the “serial passthru to COM1” check box on the Web interface)
-entercliseq	Enter a command-line interface keystroke sequence	User-defined keystroke sequence to enter the CLI while in console mode. This sequence must have at least one character and at most 15 characters. The caret symbol (^) has a special meaning in this sequence. It denotes Ctrl for keystrokes that map to Ctrl sequences (for example, ^[for the escape key and ^M for carriage return). All occurrences of ^ are interpreted as part of a Ctrl sequence. Refer to an ASCII-to-key conversion table for a complete list of Ctrl sequences. The default value for this field is “^[” (for example, Esc followed by (.
-exitcliseq	Exit a command-line interface keystroke sequence	User-defined keystroke sequence to exit the CLI. For details, see the values for the -entercliseq option in this table.

Example

```
x345RSA> srcfg
-passthru enabled
-entercliseq ^[(
-exitcliseq ^[Q
x345RSA>
```

ssl command

Syntax

```
ssl [options]
options:
-ce on | off
-se on | off
-h
```

Description

Note: Before you can enable an SSL client, a client certificate must be installed.

Use the **ssl** command to display and configure the Secure Sockets Layer (SSL) parameters.

Option	Description
-ce	Enables or disables an SSL client
-se	Enables or disables an SSL server
-h	Lists usage and options

Parameters

The following parameters are presented in the option status display for the **ssl** command and are output only from the command-line interface:

Server secure transport enable
This status display is read-only and cannot be set directly.

Server Web/CMD key status
This status display is read-only and cannot be set directly. Possible command line output values are as follows:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL server CSR key status
This status display is read-only and cannot be set directly. Possible command line output values are as follows:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL client LDAP key status
This status display is read-only and cannot be set directly. Possible command line output values are as follows as follows:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL client CSR key status
This status display is read-only and cannot be set directly. Possible command line output values are as follows:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

tcpcmdmode command

Syntax

```
tcpcmdmode [options]
options:
-t seconds
-status on|off
```

Description

Use the **tcpcmdmode** command to display and change configuration parameters for the TCP command mode sessions. You must have at least Adapter

Configuration - Networking & Security or Adapter Configuration - Advanced (Firmware Update, Restart ASM, Restore Configuration) authority level.

The following table shows the arguments for the options.

Option	Description	Values
-t	Timeout	A timeout value in seconds, up to a maximum of 4 294 967 295.
-status	Status of TCP command mode	on or off

Example

```
x345RSA> tcpcmdmode
-status on
-t 0
x345RSA>
```

timeouts command

Syntax

```
timeouts [options]
options:
-p POST_watchdog_option
-o OS_watchdog_option
-l loader_watchdog_option
-f power_off_delay_option
-n NMI_reset_delay_option
```

Description

Use the **timeouts** command to display the timeout values or change them. To display the timeouts, type `timeouts`. To change timeout values, type the options followed by the values. To change timeout values, you must have at least Adapter Configuration authority.

The following table shows the arguments for the timeout values. These values match the graduated scale pulldowns for server timeouts on the Web interface.

Option	Timeout	Units	Values
-p	POST timeout	minutes	disabled, 3.5, 4, 4.5, 5, 7.5, 10, 15, 20, 30, 60, 120
-o	Operating system timeout	minutes	disabled, 2.5, 3, 3.5, 4
-l	Loader timeout	minutes	disabled, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5, 7.5, 10, 15, 20, 30, 60, 120
-f	Power off delay	minutes	disabled, 0.5, 1, 2, 3, 4, 5, 7.5, 10, 15, 20, 30, 60, 120
-n	NMI reset delay	minutes	disabled, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4

Example

```
x345RSA> timeouts
-p 5
-o disabled
-l 3.5
-f 3
-n disabled
x345RSA> timeouts -o 2.5 -n 1
ok
```

```
x345RSA> timeouts
-p 5
-o 2.5
-l 3.5
-f 3
-n 1
```

users command

Syntax

```
users [options]
options:
-user number
-n username
-p password
-a authority level
```

Description

Use the **users** command to access all user accounts and their authority levels, and to create new user accounts and modify existing accounts.

Read the following guidelines about the **users** command:

- User numbers must be from 1 to 12, inclusive.
- User names must be less than 16 characters and can only contain numbers, letters, periods, and underscores.
- Passwords must be more than 5 and fewer than 16 characters long and must contain at least one alphabetic and one nonalphabetic character.
- The authority level can be one of the following levels:
  - super (supervisor)
  - ro (read only)
  - Any combination of the following values, separated by |:

    am (User account management access)

    rca (Remote console access)

    rcvma (Remote console and virtual media access)

    pr (Remote server power/restart access)

    cel (Ability to clear event logs)

    bc (Adapter configuration [basic])

    nsc (Adapter configuration [network and security])

    ac (Adapter configuration [advanced])

Example

```
x345RSA> users
1. USERID Read/Write
Password Expires: no expiration
2. manu Read Only
Password Expires: no expiration
3. eliflippen Read Only
Password Expires: no expiration
4.  <not used>
5. jacobyackenovic custom:cel|ac
Password Expires: no expiration
6. <not used>
7. <not used>
8. <not used>
9. <not used>
10. <not used>
```

```
11. <not used>
12. <not used>
x345RSA> users -7 -n sptest -p PASSW0RD -a custom:am|rca|cel|nsc|ac
ok
x345RSA> users
1. USERID  Read/Write
Password Expires: no expiration
2. test    Read/Write
Password Expires: no expiration
3. test2   Read/Write
Password Expires: no expiration
4. <not used>
5. jacobyackenovic custom:cel|ac
Password Expires: no expiration
6. <not used>
7. sptest  custom:am|rca|cel|nsc|ac
Password Expires: no expiration
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>
x345RSA>
```

ASM control commands

The ASM control commands are as follows:

- clearcfg
- clock
- resetsp
- update

clearcfg command

Description

Use the **clearcfg** command to set the Remote Supervisor Adapter II configuration to its factory defaults. You must have at least Advanced Adapter Configuration authority to issue this command. After the configuration of the Remote Supervisor Adapter II is cleared, the Remote Supervisor Adapter II is restarted.

clock command

Syntax

```
clock [options]
options:
-d mm/dd/yyyy
-t hh:mm:ss
-g gmt offset
-dst on/off/special case
```

Description

Use the **clock** command to display the current date and time according to the ASM clock and the GMT offset. You can set the date, time, GMT offset, and daylight saving time settings.

Note the following information:

- For a GMT offset of +2 or +10, special daylight saving time settings are required.
- For +2, the daylight saving time options are as follows: off, ee (Eastern Europe), gtb (Great Britain), egt (Egypt), fle (finland).

- For +10, the daylight saving time settings are as follows: off, ea (Eastern Australia), tas (Tasmania), vlad (Vladivostok).
- The year must be from 2000 to 2089, inclusive.
- The month, date, hours, minutes, and seconds can all be single-digit values (for example, 9:50:25 instead of 09:50:25).
- GMT offset can be in the format of +2:00, +2, or 2, for positive offsets, and -5:00 or -5, for negative offsets.

Example

```
x345RSA> clock
12/12/2003 13:15:23 GMT-5:00 dst on
x345RSA> clock -d 12/31/2004
ok
x345RSA> clock
12/31/2004 13:15:30 GMT-5:00 dst on
```

resetsp command

Description

Use the **resetsp** command to restart the Remote Supervisor Adapter II or Remote Supervisor Adapter II SlimLine. You must have at least Advanced Adapter Configuration authority to be able to issue this command.

update command

Syntax

```
update -i TFTP_server_IP_address -l filename
```

Description

Use the **update** command to update the firmware on the Remote Supervisor Adapter II or Remote Supervisor Adapter II SlimLine. To use this command, you must have at least Advanced Adapter Configuration authority. The firmware file (specified by *filename*) is first transferred from the TFTP server (specified by its IP address) to the Remote Supervisor Adapter II or Remote Supervisor Adapter II SlimLine and then flashed. The **-v** option specifies verbose mode.

Note: Make sure that the TFTP server is running on the server from which the file will be downloaded.

Option	Description
-i	TFTP server IP address
-l	File name (to be flashed)
-v	Verbose mode

Example

```
x345RSA> update -v -i 192.168.70.120 -l dev.pkt
TFTP file upload successful 1253022.
Starting flash packet preparation.
Flash preparation - packet percent complete 24.
Flash preparation - packet percent complete 48.
Flash preparation - packet percent complete 72.
Flash preparation - packet percent complete 96.
Flash preparation - packet percent complete 100.
Flash operation phase starting.
Flashing - packet percent complete 34.
Flashing - packet percent complete 38.
Flashing - packet percent complete 50.
Flashing - packet percent complete 55.
Flashing - packet percent complete 80.
Flashing - packet percent complete 90.
Flash operation complete. The new firmware will become active
after the next restart of the ASM.
ok
x345RSA>
```

Note: In the verbose mode, you do not see the flashing progress in real time. You will see it after the command completes execution.

Appendix A. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This section contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your system, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system. Information about diagnostic tools is in the *Hardware Maintenance Manual and Troubleshooting Guide* or *Problem Determination and Service Guide* on the IBM *Documentation* CD that comes with your system.

  Note: For some IntelliStation models, the *Hardware Maintenance Manual and Troubleshooting Guide* is available only from the IBM support Web site.
- Go to the IBM support Web site at http://www.ibm.com/systems/support/ to check for technical information, hints, tips, and new device drivers or to submit a request for information.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the documentation that is provided with your IBM product. The documentation that comes with IBM systems also describes the diagnostic tests that you can perform. Most systems, operating systems, and programs come with documentation that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Using the documentation

Information about your IBM system and preinstalled software, if any, or optional device is available in the documentation that comes with the product. That documentation can include printed documents, online documents, readme files, and help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to http://www.ibm.com/systems/support/ and follow the instructions. Also, some documents are available through the IBM Publications Center at http://www.ibm.com/shop/publications/order/.

Getting help and information from the World Wide Web

On the World Wide Web, the IBM Web site has up-to-date information about IBM systems, optional devices, services, and support. The address for IBM System x™ and xSeries® information is http://www.ibm.com/systems/x/. The address for IBM BladeCenter information is http://www.ibm.com/systems/bladecenter/. The address for IBM IntelliStation® information is http://www.ibm.com/intellistation/.

You can find service information for IBM systems and optional devices at http://www.ibm.com/systems/support/.

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with System x and xSeries servers, BladeCenter products, IntelliStation workstations, and appliances. For information about which products are supported by Support Line in your country or region, see http://www.ibm.com/services/sl/products/.

For more information about Support Line and other IBM services, see http://www.ibm.com/services/, or see http://www.ibm.com/planetwide/ for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Hardware service and support

You can receive hardware service through IBM Services or through your IBM reseller, if your reseller is authorized by IBM to provide warranty service. See http://www.ibm.com/planetwide/ for support telephone numbers, or in the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

IBM Taiwan product service

台灣IBM產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

IBM Taiwan product service contact information:
IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
Taipei, Taiwan
Telephone: 0800-016-888

Appendix B. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product, and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

Active Memory
Active PCI
Active PCI-X
AIX
Alert on LAN
IBM
IBM (logo)
IBM Global Network
IntelliStation
Netfinity
TechConnect
Tivoli
Tivoli Enterprise
Update Connector
Wake on LAN

BladeCenter
Chipkill
e-business logo
@server
FlashCopy
i5/OS
Predictive Failure Analysis
ServeRAID
ServerGuide
ServerProven
System x
XA-32
XA-64
X-Architecture
XpandOnDemand
xSeries

Intel, Intel Xeon, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Adaptec and HostRAID are trademarks of Adaptec, Inc., in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Red Hat, the Red Hat “Shadow Man” logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Important notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard disk drive bays with the largest currently supported drives that are available from IBM.

Maximum memory might require replacement of the standard memory with an optional memory module.

IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven®, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

IBM makes no representations or warranties with respect to non-IBM products. Support (if any) for the non-IBM products is provided by the third party, not IBM.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Index

Part Number: 43W7827

Printed in USA

(1P) P/N: 43W7827